

PATENT

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of

Renan ABGRALL et al.

Conf. 6961

Application No. 10/536,493

Group 2887

Filed May 25, 2005

Examiner Kumiko KOYAMA

SECURE ELECTRONIC ENTITY INTEGRATING LIFE SPAN MANAGEMENT OF AN
OBJECT

DECLARATION UNDER 37 CFR 1.131

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

July 8, 2009

Sir:

I, Gérald Galan, declare that:

1. I am the person in charge of intellectual property matters at Oberthur Card Systems SA, the assignee of the subject application, which has since been renamed Oberthur Technologies.

2. Prior to November 7, 2002, the invention as described and claimed in the subject application was completed in France, a WTO country, as evidenced by the following:

a. Prior to November 7, 2002, the French Attorneys who are handling the corresponding French application, forwarded to me a first draft patent application (in French) covering the subject matter described and claimed in the subject application, which I promptly reviewed as part of my regular work load. A copy of the order letter, French draft application and an English

translation of the latter are submitted herewith in support thereof.

b. I made observations as part of my regular work load on this first draft patent application and on four further draft patent applications provided by the French Attorneys, each time taking into account my observations on the previous draft patent application, the maximum time elapsed between two subsequent draft patent applications being two weeks.

c. After I approved the last draft application, the above-noted French attorneys promptly filed the corresponding French application 02/14768 on November 25, 2002, which fully supports the subject matter described and claimed in the subject application.

The undersigned declares further that all statements made herein of HIS own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.



Gérald Galan

July 8th 2003

Date

Conseils en Propriété Industrielle European Patent and Trademark Attorneys

Boîte Postale 966 75829 Paris Cedex 17
Tél. : 01 53 81 17 00 - Fax : 01 53 81 17 17 - Email : infos@bonnet-thirion.com
N° Intracommunautaire FR 12 353 616 022

MARC SANTARELLI Δ • ▽
Ing. des Arts & Manufactures
Licencié en Droit

LUC SANTARELLI Δ • ▽
Ing. Elec. E.P.F.L.
Maître en Droit

HERBERT LEWITTER Δ • ▽
B. Mech., Jur., D., Dipl. C.E.I.P.I.
U.S. Patent Attorney

JOËL BARBIN LE BOURHIS Δ • ▽
Ing. INSA
Dipl. C.E.I.P.I.

G. FOLDES Δ • ▽
Ing. I.E.G.
Licencié en Sciences

L. JULIEN-RAES Δ • ▽
Docteur en Droit
D.E.S. droit international

B. QUANTIN Δ • ▽
Ing. des Arts & Manufactures
Dr. es. Sc. Phys./Chim.

LEPLELLETIER-BEAUFOND Δ • ▽
Ing. E.C.A.M.
Dipl. I.E.F.S.I.

Consultants

A.M. DORLAND Δ • ▽
Ing. E.S.C.P.I.
Dipl. C.E.I.P.I.

H. TOURNIER Δ
Ing. des Arts & Manufactures
FORSINI-REMY Δ • ▽
Ing. Civil des mines (Nancy)

R. LOUISET
Ing. E.N.S.M.M.

Ⓢ J.L. HARTMANN Δ • ▽
Ing. E.C.L.

Administration
Brevets & Modèles J.J. PACAUD
Signes E. POULET
M. LAGARDE
N. CORDILLOT

Services Juridiques Legal Department

M. GEORGE Δ • ▽
D.E.A. Droit privé

R. COMBES Δ • ▽
D.E.S.S.P.I.
Dipl. C.E.I.P.I.

Administration
 Marques/Trademarks M. POUCHIN
 Brevets/Trademarks C. LEVIONNOIS

Administration & Finance M. MINOUSTCHINE
Computer system J.J. PACAUD
A. POUCHIN

Δ Conseil en Propriété Industrielle /
Intellectual property Attorney
* Mandataire Européen /
European Patent Attorney
▽ Conseil européen en Marques /
European Trademark Attorney

Monsieur Gérard GALAN
OBERTHUR CARD SYSTEMS SA
25 rue Auguste Blanche
B.P. 133
92800 PUTEAUX

PAR TELECOPIE

(28 pages)
01.41.38.17.02

V/Réf. : GG/GG/02/278 CSP 0207

N/Réf. : BIF114644/FR – MR/alg

Objet : CSP0207 – "Gestion du temps de vie d'un objet dans la carte"
Projet de demande de brevet national français
à déposer au nom de OBERTHUR CARD SYSTEMS SA

Inventeurs : Renan ABGRALL, Bernard GEFFROTIN

Cher Monsieur,

Nous avons le plaisir de vous transmettre ci-joint copie d'un premier projet de demande de brevet (description, revendications, abrégé et dessins informels) destiné à couvrir l'invention en objet.

Nous vous invitons à l'examiner attentivement et à nous faire part à votre plus proche convenance de vos commentaires.

En particulier, nous souhaiterions savoir si la durée de vie de l'objet doit s'entendre comme une durée totale d'utilisation effective de l'objet, ou bien comme une période de temps indépendante de la durée effective d'utilisation de l'objet (qui pourrait alors "se périmier" sans même avoir été utilisé).

Dans l'attente de vos observations, nous vous souhaitons bonne réception des présentes et vous adressons, Cher Monsieur, nos meilleures salutations.

CABINET BONNET-THIRION

Muriel ROSENBERG

P.J. projet de demande de brevet (description : pages 1 à 21 ; revendications : pages 22 à 24 ; abrégé descriptif : 1 page ; dessins : 2 planches informelles)

En association avec le Cabinet RINUY-SANTARELLI, Société Anonyme de Conseils en Propriété Industrielle
Cabinet BONNET-THIRION : Société anonyme de Conseils en Propriété Industrielle au capital de 2 000 000 FF
Siège social : 12, avenue de la Grande Armée 75017 PARIS - RCS 353 616 022
Ⓢ TOULOUSE : Immeuble Innopolis A - B.P. 388-31314 LABEGE Cedex - Tél. : 05 61 00 75 30 - Fax : 05 61 00 75 39

 *** RAPPORT TX ***

EMISSION OK

TX/RX N° 2629
 TEL. CORRESPONDANT 01 41 38 17 02
 SOUS-ADRESSE
 ID CORRESPONDANT
 HEURE DEBUT
 DUREE 09'00
 PGS. 28
 RESULTAT OK

Cabinet fondé/established in
 1852 par/by Charles THIRION

CABINET BONNET - THIRION

Conseils en Propriété Industrielle
 European Patent and Trademark Attorneys

Boîte Postale 966 75829 Paris Cedex 17
 Tél. : 01 53 81 17 00 - Fax : 01 53 81 17 17 - Email : infos@bonnet-thirion.com
 N° Intracommunautaire FR 12 353 616 022

M. C. SANTAFELLI A + D
 Ing. des Arts & Manufactures
 Licencié en Droit

L. C. SANTAFELLI A + D
 Ing. Elec. E.P.F.L.
 Maître en Droit

HERBERT LEWINTER A + D
 B. Scs., Jur., D., Dipl. C.E.I.P.I.
 U.S. Patent Attorney

JOËL BAILLEUX LE BOUILLON A + D
 Ing. INSA
 Dipl. C.E.I.P.I.

G. FOLDES A + D
 Ing. I.E.G.
 Licencié en Sciences

L. JULIEN-RAES A + D
 Docteur en Droit
 D.E.S. droit International

B. QUANTIN A + D
 Ing. des Arts & Manufactures
 Dr. es. Sc. Phys./Chim.

J. LEPELLENIER-BEAUJON A + D
 Ing. I.C.A.M.
 Dipl. I.F.E.S.I.

Conseillers

H. TOURNIER A
 Ing. des Arts & Manufactures

FORSINI-REMY A + D
 Ing. Civil des Mines (Nancy)

R. LOUISET
 Ing. E.N.S.M.M.

J. L. HARTMANN A + D
 Ing. C.C.I.

Administration
 Représentants & Mandataires J.J. PACAUD
 Mandataires & Représentants J. POULET
 M. JAGARDE
 N. CORDILLON

Services Juridiques
 Legal Department
 M. GEORGE A + D

PAI TELECOPIE
 (28 pages)
 01. 1.38.17.02

Monsieur Gérard GALAN
 OBERTHUR CARD SYSTEMS SA
 25 rue Auguste Blanche
 B.P. 133
 92800 PUTEAUX

V/Réf. : GG/GG/02/278 CSP 0207
 N/Réf. : BIF114644/FR - MR/alg

Objet : CSP0207 - "Gestion du temps de vie d'un objet dans la carte"
 Projet de demande de brevet national français
 à déposer au nom de OBERTHUR CARD SYSTEMS SA

Inventeurs : Renan ABGRALL, Bernard GEFROTIN

Cher Monsieur,

Nous avons le plaisir de vous transmettre ci-joint copie d'un premier projet de demande de brevet (description, revendications, abrégé et dessins informels) destiné à couvrir l'invention en objet.

Nous vous invitons à l'examiner attentivement et à nous faire part à votre plus proche connaissance de vos commentaires.

En particulier, nous souhaiterions savoir si la durée de vie de l'objet doit s'entendre comme une durée totale d'utilisation effective de l'objet, ou bien comme une période de temps indépendante de la durée effective d'utilisation de l'objet (qui pourrait alors "se déprimer" sans même avoir été utilisé).

Dans l'attente de vos observations, nous vous souhaitons bonne réception des présentes et vous adressons, Cher Monsieur, nos meilleures salutations.

ENTITE ELECTRONIQUE SECURISEE INTEGRANT LA GESTION DU TEMPS DE VIE D'UN OBJET

5 L'invention se rapporte à une entité électronique sécurisée adaptée à mémoriser au moins un objet et a notamment pour objet un perfectionnement apporté à une telle entité électronique pour que celle-ci puisse effectuer une gestion d'un temps de vie attribué à l'objet, qui s'écoule à partir d'une date de référence associée à cet objet.

10 On entend ici une gestion du temps "dans" l'entité électronique au sens où cette gestion est indépendante de tout système extérieur de mesure du temps, qu'il s'agisse par exemple d'un générateur de signal d'horloge ou de tout autre moyen de mesure du temps situé à l'extérieur par rapport à l'entité électronique.

Ces spécificités permettent de rendre relativement inviolable l'entité électronique objet de la présente invention.

15 L'invention peut s'appliquer à toute entité électronique sécurisée, comme, par exemple, une carte à microcircuit sécurisée, comportant des moyens lui permettant d'être couplée au moins temporairement à une source d'énergie électrique pour la mise en œuvre au moins d'une opération. L'invention peut notamment permettre de gérer la durée de vie de la carte elle-même ou d'objets
20 contenus dans la carte, en l'absence de source permanente d'alimentation en énergie.

La sécurité d'un objet mémorisé dans une entité électronique (par exemple une carte à microcircuit telle qu'une carte bancaire ou une carte de contrôle d'accès ou autre) peut être améliorée s'il est possible de prendre en
25 compte le temps qui s'est écoulé depuis une date de référence liée à cet objet, que l'objet soit le microcircuit de la carte elle-même ou qu'il soit contenu dans la carte, comme c'est le cas pour un code secret (code PIN), un fichier de données, une fonction cryptographique (clé, certificat), une application ou encore des droits d'accès.

30 Il existe une grande variété d'attaques possibles contre les cartes à microcircuit. Certaines de ces attaques ont pour but de retrouver les secrets qui sont conservés dans la mémoire du microcircuit ou de modifier le comportement normal de la carte afin d'en tirer profit. Par exemple, DPA (analyse de puissance

différentielle, en anglais "*Differential Power Analysis*"), SPA (analyse de puissance simple, en anglais "*Simple Power Analysis*"), EMA (analyse électromagnétique, en anglais "*ElectroMagnetic Analysis*"), DEMA (analyse électromagnétique différentielle, en anglais "*Differential ElectroMagnetic Analysis*"), ou encore DFA (analyse d'erreur différentielle, en anglais "*Differential Fault Analysis*") sont des appellations bien connues de telles attaques, dites non intrusives, car n'entraînant pas la destruction de la carte.

Néanmoins, en ce qui concerne les cartes à microcircuit connues, la notion de temps est le plus souvent apportée par l'extérieur (comme, de façon classique, par un signal d'horloge extérieur), ce qui rend plus facilement réalisables les attaques mentionnées ci-dessus.

La présente invention a pour but de remédier aux inconvénients précités, en empêchant un "attaquant" ou un fraudeur d'utiliser de façon abusive une entité électronique sécurisée, ou un ou plusieurs objets mémorisés dans celle-ci. Pour ce faire, la présente invention intègre dans l'entité électronique la gestion du temps de vie attribué à ce ou ces objets, voire à l'entité électronique elle-même.

Dans ce but, l'invention propose une entité électronique sécurisée comportant une unité adaptée à mémoriser au moins un objet, remarquable en ce qu'elle contient une unité de mesure du temps qui s'écoule à partir d'une date de référence associée à cet objet et en ce qu'elle comporte :

- une unité de mémorisation d'une durée de vie attribuée à l'objet, l'unité de mémorisation coopérant avec l'unité de mesure du temps de façon à comparer, à chaque utilisation de l'objet, le temps écoulé et la durée de vie et
- une unité de mise à jour et d'invalidation, pour mettre à jour la durée de vie ou rendre l'objet temporairement ou définitivement inutilisable s'il résulte de la comparaison précitée que le temps écoulé atteint ou dépasse la durée de vie.

Conformément à l'invention, les moyens permettant de déterminer le temps qui s'écoule à partir de la date de référence se situent dans l'entité électronique, ce qui permet d'augmenter sa sécurisation.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps qui s'écoule à partir de la date de référence même lorsque l'entité électronique n'est pas alimentée par une source d'énergie extérieure.

5 Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps qui s'écoule à partir de la date de référence même lorsque l'entité électronique n'est pas alimentée électriquement.

Avantageusement, l'unité de mesure du temps est adaptée à fournir une mesure du temps qui s'écoule à partir de la date de référence indépendamment de tout signal d'horloge extérieur.

10 En ce sens, l'entité électronique est autonome, à la fois du point de vue de la mesure du temps et du point de vue de l'alimentation électrique.

En variante, on peut bien entendu prévoir une pile et/ou une horloge dans l'entité électronique.

15 L'unité de mesure du temps peut comporter un moyen de comparaison de deux dates, une date étant, de façon générale, une expression du temps courant et ces deux dates s'entendant ici comme deux instants définis par rapport à une même référence temporelle, laquelle est par exemple la date de référence associée à l'objet dont l'entité électronique contrôle la durée de vie. Le moyen de comparaison peut comparer la date courante, soit directement à la date de
20 référence de l'objet, ce qui permet de déduire directement la durée de vie restante de l'objet, soit à une autre date, telle que la date de la dernière utilisation de l'objet.

L'unité de mémorisation de la durée de vie comporte avantageusement une entité sécurisée et peut être située dans ou hors de l'entité électronique.

25 Comme mentionné en introduction, à titre d'exemples non limitatifs, l'objet peut être un microcircuit, un code secret, un fichier ou un système de fichiers, une fonction cryptographique telle qu'une clé ou un certificat, une application ou encore des droits d'accès. La date de référence associée à l'objet peut être la date à laquelle l'objet a été créé dans l'entité électronique.

30 Dans un mode de réalisation préféré de la présente invention, l'entité électronique sécurisée comporte au moins un sous-ensemble comprenant :

un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ce composant capacitif à une source d'énergie électrique pour être chargé par la source d'énergie électrique et un moyen de mesure de la charge résiduelle du composant capacitif, cette charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique.

Dans ce cas, le composant capacitif du sous-ensemble précité ne peut être chargé que lorsque l'entité électronique sécurisée est couplée à la source d'énergie électrique. Cette dernière peut être extérieure à l'entité électronique sécurisée, mais ce n'est pas impératif : en variante, on peut prévoir d'alimenter l'entité électronique par une pile disposée dans ou sur celle-ci.

L'entité électronique pourra être pourvue d'un moyen de commutation pour découpler le composant capacitif de la source d'énergie électrique, cet événement initialisant la mesure du temps.

Plus généralement, la mesure du temps, c'est-à-dire la variation de charge du composant capacitif, commence dès que, après avoir été chargé, celui-ci se trouve électriquement isolé de tout autre circuit et ne peut plus se décharger qu'à travers son propre espace diélectrique.

Cependant, même si, physiquement, la charge résiduelle mesurée est liée à l'intervalle de temps écoulé entre l'isolement de l'élément capacitif et une mesure donnée de sa charge résiduelle, un intervalle de temps mesuré peut être déterminé entre deux mesures, la première mesure déterminant en quelque sorte une charge résiduelle de référence. Le moyen de mesure de la charge résiduelle du composant capacitif est mis en œuvre lorsqu'on désire connaître un temps écoulé.

Le composant capacitif est chargé au cours d'une utilisation de l'objet dont l'entité électronique contrôle la durée de vie, cette "utilisation" s'entendant au sens le plus large et incluant par exemple la création de l'objet. Le moyen de mesure de la charge résiduelle est mis en œuvre au cours d'une telle utilisation pour fournir une information au moins en partie représentative du temps qui s'est écoulé depuis la dernière utilisation.

Par ailleurs, l'invention permet en outre à l'entité électronique sécurisée de continuer à mesurer le temps écoulé, même après que l'entité électronique a été temporairement alimentée en courant et qu'elle se trouve ensuite dépourvue de toute nouvelle alimentation électrique. L'invention ne nécessite donc pas
5 d'utiliser une source d'énergie électrique en permanence.

Le moyen de mesure de la charge résiduelle peut être compris dans l'unité de mesure du temps mentionnée plus haut.

Dans le mode préféré de réalisation, le moyen de mesure de la charge résiduelle comprend un transistor à effet de champ dont la grille est connectée à
10 une borne du composant capacitif, c'est-à-dire à une "armature" d'une capacité.

Une telle capacité peut être réalisée en technologie MOS et son espace diélectrique peut alors être constitué par un oxyde de silicium. Dans ce cas, il est avantageux que le transistor à effet de champ soit réalisé également en technologie MOS. La grille du transistor à effet de champ et l'"armature" du
15 composant capacitif MOS sont reliées et constituent une sorte de grille flottante qui peut être connectée à un composant permettant d'injecter des porteurs de charge.

On peut aussi faire en sorte qu'il n'existe aucune connexion électrique à proprement parler avec l'environnement extérieur. La connexion de la grille flottante peut être remplacée par une grille de contrôle (électriquement isolée)
20 qui vient charger la grille flottante, par exemple par effet tunnel ou par "porteurs chauds". Cette grille permet de faire transiter des porteurs de charge vers la grille flottante commune au transistor à effet de champ et au composant capacitif. Cette technique est bien connue des fabricants de mémoires de type
25 EPROM ou EEPROM.

Le transistor à effet de champ et le composant capacitif peuvent constituer une unité intégrée dans un microcircuit compris dans l'entité électronique sécurisée ou faisant partie d'un autre microcircuit logé dans la même entité électronique sécurisée.

30 Pendant certaines opérations liées à une utilisation de l'objet dont la durée de vie est contrôlée par l'entité électronique sécurisée, lorsque l'entité électronique sécurisée est encore couplée à une source d'énergie électrique extérieure, le composant capacitif est chargé à une valeur prédéterminée,

connue ou mesurée et mémorisée, et le moyen de mesure de la charge résiduelle est relié à une borne de ce composant capacitif.

5 A la fin d'une série d'opérations correspondant à une période d'utilisation de l'objet, le moyen de mesure de la charge résiduelle, notamment le transistor à effet de champ, n'est plus alimenté mais sa grille reliée à la borne du composant capacitif est portée à une tension correspondant à la charge de celui-ci.

10 Pendant toute la période de temps qui sépare la date de référence associée à l'objet de la date de son utilisation courante, le composant capacitif se décharge lentement au travers de son propre espace diélectrique de sorte que la tension appliquée sur la grille du transistor à effet de champ diminue progressivement.

15 Au moment où l'entité électronique est à nouveau connectée à une source d'énergie électrique pour la mise en œuvre d'une nouvelle opération liée à une nouvelle période d'utilisation de l'objet, une tension électrique est appliquée entre le drain et la source du transistor à effet de champ. Ainsi, un courant électrique allant du drain vers la source (ou dans le sens contraire selon les cas) est engendré et peut être recueilli et analysé.

20 La valeur du courant électrique mesuré dépend des paramètres technologiques du transistor à effet de champ et de la différence de potentiel entre le drain et la source, mais aussi de la tension entre la grille et le substrat. Le courant dépend donc des porteurs de charge accumulés dans la grille flottante commune au transistor à effet de champ et au composant capacitif. Par conséquent, ce courant de drain est aussi représentatif du temps qui s'est écoulé, lors de l'utilisation de l'objet, entre la date de référence et la date courante.

25 Le courant de fuite d'une telle capacité dépend bien sûr de l'épaisseur de son espace diélectrique mais également de tout autre paramètre dit technologique tel que les longueurs et surfaces de contact des éléments du composant capacitif. Il faut également prendre en compte l'architecture tridimensionnelle des contacts de ces parties, qui peut induire des phénomènes modifiant les paramètres du courant de fuite (par exemple, modification de la valeur de la capacité dite tunnel). Le type et la quantité des dopants et des

30

défauts peuvent être modulés pour modifier les caractéristiques du courant de fuite.

5 Les variations de température ont aussi une influence, plus précisément la moyenne des apports d'énergie calorifique appliqués à l'entité électronique sécurisée pendant le temps d'utilisation de l'objet. En fait, tout paramètre intrinsèque à la technologie MOS peut être source de modulation du processus de la mesure du temps.

10 Avantageusement, l'épaisseur de la couche isolante du transistor à effet de champ est notablement supérieure (par exemple environ trois fois supérieure) à l'épaisseur de la couche isolante du composant capacitif.

Quant à l'épaisseur de la couche isolante du composant capacitif, elle est avantageusement comprise entre 4 et 10 nanomètres.

15 Pour obtenir une information sensiblement uniquement représentative du temps, on peut prévoir, dans une variante de réalisation, au moins deux sous-ensembles tels que définis ci-dessus, exploités "en parallèle". Les deux composants capacitifs sensibles à la température sont définis avec des fuites différentes, toutes choses égales par ailleurs, c'est-à-dire que leurs espaces diélectriques (épaisseur de la couche d'oxyde de silicium) ont des épaisseurs différentes.

20 A cet effet, selon une disposition avantageuse de l'invention, l'entité électronique définie ci-dessus est remarquable en ce qu'elle comporte :

au moins deux sous-ensembles précités comprenant chacun :

25 un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ce composant capacitif à une source d'énergie électrique pour être chargé par cette source d'énergie électrique et

30 un moyen de mesure de la charge résiduelle du composant capacitif, cette charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique,

ces sous-ensembles comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs, et en ce que l'entité électronique sécurisée comporte en outre :

des moyens de traitement des mesures des charges résiduelles respectives de ces composants capacitifs, pour extraire de ces mesures une information sensiblement indépendante des apports calorifiques appliqués à l'entité électronique sécurisée pendant le temps écoulé à partir de la date de référence.

Par exemple, les moyens de traitement peuvent comporter un tableau de valeurs de temps mémorisées, ce tableau étant adressé par ces mesures respectives. Autrement dit, chaque couple de mesures désigne une valeur de temps mémorisée indépendante de la température et des variations de température pendant la période mesurée. L'entité électronique comporte avantageusement une mémoire associée à un microprocesseur et une partie de cette mémoire peut être utilisée pour mémoriser le tableau de valeurs.

En variante, les moyens de traitement peuvent comporter un logiciel de calcul programmé pour exécuter une fonction prédéterminée permettant de calculer l'information temps, sensiblement indépendante des apports calorifiques, en fonction des deux mesures précitées.

L'invention est particulièrement adaptée à s'appliquer aux cartes à microcircuit. L'entité électronique sécurisée peut être une carte à microcircuit, ou en comprendre une, ou encore être d'un autre type, par exemple, être une carte PCMCIA (architecture internationale de cartes-mémoire d'ordinateurs individuels, en anglais "*Personal Computer Memory Card International Architecture*").

L'invention est en outre remarquable par son niveau d'intégration.

D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit de modes particuliers de réalisation, donnés à titre d'exemples non limitatifs. La description est faite en référence aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 est un synoptique représentant, dans un mode particulier de réalisation, une entité électronique sécurisée conforme à la présente invention ;

- la figure 2 est un schéma-bloc d'une carte à microcircuit à laquelle peut s'appliquer l'invention, dans un mode particulier de réalisation ;

- la figure 3 est un schéma de principe d'un sous-ensemble que l'entité électronique sécurisée peut comporter dans un mode particulier de réalisation ; et

5 - la figure 4 est un schéma-bloc d'une variante du mode de réalisation des figures 1 et 2.

Comme le montre la **figure 1**, dans un mode particulier de réalisation, une entité électronique sécurisée 11 conforme à la présente invention comporte une mémoire non volatile 23, par exemple du type EEPROM, mémorisant des données relatives à au moins un objet, tel qu'un microcircuit, un code secret (PIN
10 ou autre), un fichier ou un système de fichiers, une clé de cryptage ou un certificat, une application, ou encore des droits d'accès.

L'entité électronique 11 contient une unité 18 de mesure du temps qui s'écoule à partir d'une date de référence Dref associée à l'objet mémorisé dans l'EEPROM 23. Cette date de référence peut par exemple être la date de création
15 de l'objet dans la carte.

L'unité 18 de mesure du temps est indépendante de tout système extérieur de mesure du temps, qu'il s'agisse par exemple d'un générateur de signal d'horloge ou de tout autre moyen de mesure du temps situé à l'extérieur par rapport à la carte.

20 L'entité électronique sécurisée 11 comporte également une unité 19 de mémorisation de plusieurs paramètres définissant l'objet dont on veut gérer le temps de vie dans l'entité électronique sécurisée :

- un identifiant Id de l'objet,
- la date de référence Dref précitée, et
- 25 - un temps de vie V attribué à l'objet et déterminé au préalable.

Les opérations de création d'un objet mettent bien entendu en œuvre des mécanismes sécuritaires pour protéger la donnée "durée de vie" V.

L'unité de mémorisation 19 peut ne constituer qu'une seule et même mémoire avec l'EEPROM 23. L'unité de mémorisation 19 est avantageusement
30 une mémoire sécurisée de l'entité électronique 11, cette mémoire étant notamment non accessible de l'extérieur. En variante, on peut envisager de situer l'unité de mémorisation 19 hors de l'entité électronique sécurisée 11, dans une entité sécurisée extérieure. Dans ce dernier cas, la valeur de la durée de vie

V est reçue de l'extérieur, de la part d'un tiers dit "de confiance" (autorité habilitée), par l'entité électronique sécurisée 11, par l'intermédiaire d'un protocole sécurisé (i.e. mettant en œuvre des moyens cryptographiques) et est mémorisée au moins temporairement dans une zone sécurisée de l'entité électronique 11.

5 L'entité électronique sécurisée 11 comporte en outre une unité 21 de mise à jour et d'invalidation, commandée par l'unité 18 de mesure du temps.

Conformément à la présente invention, l'unité de mémorisation 19 coopère avec l'unité 18 de mesure du temps de façon à comparer, à chaque utilisation de l'objet, le temps écoulé et la durée de vie V.

10 Si, après comparaison du temps écoulé et de la durée de vie V, il apparaît que la durée de vie est atteinte ou dépassée, l'unité 21 de mise à jour et d'invalidation agit sur l'objet, pour, soit mettre à jour sa durée de vie V dans l'unité de mémorisation 19, afin de prolonger le temps de vie de l'objet, moyennant la mise en œuvre de mécanismes sécuritaires, soit inhiber
15 temporairement le fonctionnement de l'objet, pendant une période de temps prédéterminée, voire rendre l'objet définitivement inutilisable.

On peut prévoir dans la mémoire de l'entité électronique sécurisée 11 une région (comprenant par exemple un fichier) contenant la date, par exemple en secondes, à partir de la date de référence Dref.

20 Dès lors, avant d'autoriser une nouvelle utilisation de l'objet, il est prévu de comparer la date de l'utilisation courante avec la date de référence Dref. Si la différence entre les deux dates est égale ou supérieure à la durée de vie V, l'unité 21 de mise à jour et d'invalidation entre en action.

L'invention compte de nombreuses applications possibles, parmi
25 lesquelles on peut citer :

- la limitation de la durée de vie d'une carte à microcircuit en fonction de la durée du contrat souscrit par son utilisateur, de façon à garantir qu'aucun usage détourné et frauduleux de la carte n'ait lieu au-delà de la durée d'utilisation prévue ;

30 - la limitation, de façon analogue, de la durée de vie d'un système de fichiers ;

- la commande d'un changement périodique, par l'utilisateur, du code confidentiel lié à l'utilisation de l'entité électronique sécurisée ;

- la définition d'une date limite de validité pour des données contenues dans un fichier, au-delà de laquelle la lecture de ces données sera rendue impossible ou du moins sera accompagnée d'une mise en garde à l'attention de l'utilisateur ;

5 - la détection de la fin de la validité d'une application, liée par exemple à un événement sportif, culturel ou artistique limité dans le temps, au-delà de laquelle cette application sera automatiquement supprimée ;

 - la définition d'une date d'échéance pour une période d'essai gratuit d'une version d'évaluation en ligne d'un logiciel, au-delà de laquelle les droits d'utilisation du logiciel pourront être prolongés (moyennant la mise en œuvre d'un mécanisme sécuritaire), après paiement par l'utilisateur ;

10

 - la gestion de droits d'accès électronique à un morceau musical, un film ou autre, via Internet, sous forme d'abonnement forfaitaire d'une durée fixée à l'avance (par exemple, un mois) ou en fonction de la durée effective d'utilisation de ces droits d'accès (par exemple, dix heures d'écoute) ;

15

- etc.

Dans le dernier exemple d'application mentionné ci-dessus, un utilisateur souhaite par exemple accéder pour une durée définie au contenu du site Internet d'un éditeur de contenu musical. Il achète à cet effet des droits d'accès au contenu musical pour une durée déterminée, par exemple quatre heures. Après

20

vérification, l'éditeur envoie à l'entité électronique sécurisée de l'utilisateur un message sécurisé d'ouverture de droits d'écoute pour la durée prévue. A réception de ce message, l'entité électronique sécurisée crée dans sa mémoire un objet "droit d'écoute" et initialise la durée de vie V avec la valeur choisie, ici

25

quatre heures.

A la première utilisation de l'objet, c'est-à-dire lors du premier accès au contenu musical, l'entité électronique sécurisée vérifie la présence de l'objet "droit d'écoute" et mémorise la date de début d'écoute. L'utilisateur accède ensuite au contenu musical. A chaque demande d'un secret de décryptage,

30

l'entité électronique sécurisée vérifie la présence de l'objet "droit d'écoute" et sa validité, en fonction du temps actualisé. Si la différence entre la date courante et la date de référence (qui est ici la date de début d'écoute) est supérieure à quatre heures, alors le droit est toujours valable et l'entité électronique sécurisée

fournit le secret qui permet de décrypter le contenu musical. En revanche, si cette différence est égale ou supérieure à quatre heures, le droit n'est plus valable et le secret de décodage n'est plus fourni. En outre, l'entité électronique peut invalider temporairement l'objet "droit d'écoute", voire le détruire.

5 En cas d'arrêt d'utilisation de l'objet "droit d'écoute" par l'utilisateur avant la fin des droits, la durée de vie de cet objet est mise à jour en fonction du temps restant : la nouvelle valeur de la durée de vie est égale à la durée de vie précédente, diminuée de la date courante ainsi que de la date de début d'écoute.

10 Dans un autre exemple d'application de l'invention, dans le domaine des télécommunications mobiles, l'entité électronique sécurisée peut être une carte à puce du type carte SIM et l'objet peut être une application dite SAT ("*SIM Application Toolkit*", défini notamment par la norme GSM 03.48). Les applications peuvent être chargées au moment de la personnalisation de la carte SIM, ou être téléchargées, soit en utilisant la technologie SMS (service de messages courts, en anglais "*Short Message Service*"), également définie par la

15 norme GSM précitée, soit via un lecteur connecté à un ordinateur lui-même connecté à un centre de gestion de cartes.

 L'entité électronique gère un tableau d'applications SAT contenant, pour chaque application, un identifiant AID de l'application, une date de référence (qui

20 est par exemple la date de création de l'application) et la durée de vie de l'application.

 A chaque déclenchement de l'application, la carte SIM détermine grâce au compteur de temps si l'application est toujours valable. Si ce n'est pas le cas, c'est-à-dire si la différence entre la date courante et la date de création de

25 l'application est égale ou supérieure à la durée de vie de l'application, la carte envoie une commande administrative de type Delete_application(AID) et met à jour le tableau d'applications SAT.

 La **figure 2** illustre une entité électronique sécurisée 11 conforme à la présente invention, dans un mode particulier de réalisation où cette entité est

30 une carte à microcircuit. L'entité électronique sécurisée 11 comporte une unité 12 lui permettant d'être couplée à une source d'énergie électrique extérieure 16.

 Dans le mode particulier de réalisation représenté, l'entité électronique sécurisée 11 comporte des plages de raccordement métalliques susceptibles

d'être connectées à une unité formant un lecteur de carte. Deux de ces plages de raccordement 13a, 13b sont réservées à l'alimentation électrique du microcircuit, la source d'énergie électrique étant logée dans un serveur ou autre dispositif auquel l'entité électronique sécurisée est momentanément raccordée. Ces plages de raccordement peuvent être remplacées par une antenne logée dans l'épaisseur de la carte et susceptible de fournir au microcircuit l'énergie électrique nécessaire à son alimentation tout en assurant la transmission bidirectionnelle de signaux radiofréquence permettant les échanges d'informations. On parle alors de technologie sans contact.

Le microcircuit comprend un microprocesseur 14 associé de façon classique à une mémoire 15.

Dans un exemple particulier de réalisation, l'entité électronique sécurisée 11 comporte au moins un sous-ensemble 17 (ou est associée à un tel sous-ensemble) chargé de la mesure du temps.

Le sous-ensemble 17, qui est représenté plus en détail sur la **figure 3**, est donc logé dans l'entité électronique sécurisée 11. Il peut faire partie du microcircuit et être réalisé dans la même technologie d'intégration que celui-ci.

Dans l'exemple, ce sous-ensemble 17 n'est relié à aucune source d'énergie électrique interne. Il ne peut donc être alimenté que lorsque l'entité électronique sécurisée 11 est effectivement couplée à un serveur ou à un lecteur de carte, comportant une telle source d'énergie électrique. Cependant, si l'entité électronique sécurisée 11 doit être alimentée en permanence, le sous-ensemble 17 qui est chargé de la mesure du temps peut être alimenté ou non via un module de commutation permettant de coupler l'entité électronique sécurisée 11 à la source d'énergie électrique ou de l'isoler de celle-ci. Un tel module de commutation est par exemple partie intégrante du microprocesseur 14, ou constitué par des éléments de commutation gérés par le microprocesseur 14.

Le sous-ensemble 17 comprend un composant capacitif 20 présentant une fuite au travers de son espace diélectrique 24 et une unité 22 de mesure de la charge résiduelle de ce composant 20.

Cette charge résiduelle est au moins en partie représentative du temps écoulé après que le composant capacitif 20 a été découplé de la source

d'énergie électrique, c'est-à-dire, dans l'exemple donné ici, depuis la date de référence Dref associée à l'objet dont on cherche à contrôler la durée de vie.

5 Le composant capacitif 20 est chargé par la source d'énergie électrique extérieure au cours d'une opération liée à l'utilisation de l'objet, soit par connexion directe, comme dans l'exemple décrit, soit par tout autre moyen qui peut amener à charger la grille. L'effet tunnel est une méthode permettant de charger la grille sans connexion directe. Dans l'exemple, la charge du composant capacitif 20 est pilotée par le microprocesseur 14.

10 Dans l'exemple, le composant capacitif 20 est une capacité réalisée suivant la technologie MOS. L'espace diélectrique 24 de cette capacité est constitué par une couche d'oxyde de silicium déposée à la surface d'un substrat 26 constituant une des armatures du condensateur. Ce substrat 26 est ici connecté à la masse, c'est-à-dire à une des bornes d'alimentation de la source d'énergie électrique extérieure, lorsque celle-ci se trouve raccordée à la carte.

15 L'autre armature du condensateur est un dépôt conducteur 28a appliqué sur l'autre face de la couche d'oxyde de silicium.

Par ailleurs, l'unité 22 de mesure mentionnée précédemment comprend essentiellement un transistor 30 à effet de champ, ici réalisé suivant la technologie MOS, comme la capacité. La grille du transistor 30 est connectée à

20 une borne du composant capacitif 20. Dans l'exemple, la grille est un dépôt conducteur 28b de même nature que le dépôt conducteur 28a qui, comme indiqué ci-dessus, constitue une des armatures du composant capacitif 20.

Les deux dépôts conducteurs 28a et 28b sont reliés l'un à l'autre ou ne constituent qu'un seul et même dépôt conducteur. Une connexion 32 reliée au

25 microprocesseur 14 permet d'appliquer une tension à ces deux dépôts 28a et 28b, pendant un court intervalle de temps nécessaire pour charger le composant capacitif 20. L'application de cette tension est pilotée par le microprocesseur 14.

Plus généralement, la connexion 32 permet de charger le composant capacitif 20 à un moment choisi, sous la commande du microprocesseur 14 et

30 c'est à partir du moment où cette connexion de charge est coupée par le microprocesseur 14 (ou lorsque l'entité électronique sécurisée 11 est découplée dans son ensemble de toute source d'alimentation électrique) que la décharge du composant capacitif 20 au travers de son espace diélectrique 24 commence,

cette perte de charge électrique étant représentative du temps écoulé. La mesure du temps implique la mise en conduction momentanée du transistor 30, ce qui suppose la présence d'une source d'énergie électrique appliquée entre drain et source.

5 Le transistor 30 à effet de champ en technologie MOS comporte, outre la grille, un espace diélectrique de grille 34 séparant cette dernière d'un substrat 36 dans lequel sont définies une région de drain 38 et une région de source 39. L'espace diélectrique de grille 34 est constitué par une couche isolante d'oxyde de silicium. La connexion de source 40 appliquée à la région de source 39 est
10 reliée à la masse et au substrat 36. La connexion de drain 41 est reliée à un circuit de mesure du courant de drain qui comporte une résistance 45 aux bornes de laquelle sont connectées les deux entrées d'un amplificateur différentiel 46. La tension délivrée à la sortie de cet amplificateur est donc proportionnelle au courant de drain.

15 La grille 28b est mise en position flottante pendant le temps qui s'écoule entre deux couplages ou connexions à une source d'énergie électrique extérieure, c'est-à-dire à l'occasion de deux utilisations successives de l'objet. Autrement dit, aucune tension n'est appliquée à la grille pendant cet intervalle de temps. En revanche, puisque la grille est connectée à une armature du
20 composant capacitif 20, la tension de grille pendant cet intervalle de temps est égale à une tension qui se développe entre les bornes du composant capacitif 20 et qui résulte d'une charge initiale de celui-ci réalisée sous le contrôle du microprocesseur 14 au cours de la dernière utilisation de l'objet.

 L'épaisseur de la couche isolante du transistor 30 est notablement plus
25 grande que celle du composant capacitif 20. A titre d'exemple non limitatif, l'épaisseur de la couche isolante du transistor 30 peut être environ trois fois supérieure à l'épaisseur de la couche isolante du composant capacitif 20. Selon l'application envisagée, l'épaisseur de la couche isolante du composant capacitif 20 est comprise entre 4 et 10 nanomètres, environ.

30 Lorsque le composant capacitif 20 est chargé par la source d'énergie électrique extérieure et après que la connexion de charge a été coupée sous la commande du microprocesseur 14, la tension aux bornes du composant capacitif 20 diminue lentement au fur et à mesure que ce dernier se décharge

progressivement au travers de son propre espace diélectrique 24. La décharge au travers de l'espace diélectrique 34 du transistor 30 à effet de champ est négligeable compte tenu de l'épaisseur de ce dernier.

5 A titre d'exemple nullement limitatif, si, pour une épaisseur d'espace diélectrique donnée, on charge la grille et l'armature du composant capacitif 20 à 6 volts à un instant $t = 0$, le temps associé à une perte de charge de 1 volt, c'est-à-dire un abaissement de la tension à une valeur de 5 volts, est de l'ordre de 24 secondes pour une épaisseur de 8 nanomètres.

Pour des épaisseurs différentes, on peut dresser le tableau suivant :

10

Durée	1 heure	1 journée	1 semaine	1 mois
Epaisseur d'oxyde	8,17 nm	8,79 nm	9,17 nm	9.43 nm
Précision sur le temps	1,85 %	2,09 %	2,24 %	3,10 %

La précision dépend de l'erreur commise sur la lecture du courant de drain (0,1 % environ). Ainsi, pour pouvoir mesurer des temps de l'ordre d'une semaine, on peut prévoir une couche d'espace diélectrique de l'ordre de 9 nanomètres.

15

La figure 3 montre une architecture particulière qui utilise une connexion directe à la grille flottante (28a, 28b) pour y appliquer un potentiel électrique et donc y faire transiter des charges. On peut aussi procéder à une charge indirecte, comme mentionné précédemment, grâce à une grille de contrôle remplaçant la connexion directe, selon la technologie utilisée pour la fabrication des cellules EPROM ou EEPROM.

20

La variante de la **figure 4** prévoit trois sous-ensembles 17A, 17B, 17C, chacun associé au microprocesseur 14. Les sous-ensembles 17A et 17B comprennent des composants capacitifs présentant des fuites relativement faibles pour permettre des mesures de temps relativement longs.

25

Cependant, ces composants capacitifs sont généralement sensibles aux variations de température. Le troisième sous-ensemble 17C comporte un composant capacitif présentant un espace diélectrique très faible, inférieur à 5 nanomètres. Il est de ce fait insensible aux variations de température. Les deux

composants capacitifs des sous-ensembles 17A, 17B présentent des fuites différentes au travers de leurs espaces diélectriques respectifs.

5 En outre, l'entité électronique sécurisée comporte un module de traitement des mesures des charges résiduelles respectives présentes dans les composants capacitifs des deux premiers sous-ensembles 17A, 17B. Ce module de traitement est adapté à extraire de ces mesures une information représentative des temps et sensiblement indépendante des apports calorifiques appliqués à l'entité électronique sécurisée pendant le temps écoulé depuis la date de référence.

10 Dans l'exemple, ce module de traitement se confond avec le microprocesseur 14 et la mémoire 15. En particulier, un espace de la mémoire 15 est réservé à la mémorisation d'un tableau T à double entrée de valeurs de temps et ce tableau est adressé par les deux mesures respectives issues des sous-ensembles 17A et 17B. Autrement dit, une partie de la mémoire comporte
15 un ensemble de valeurs de temps et chaque valeur correspond à un couple de mesures résultant de la lecture du courant de drain de chacun des deux transistors des sous-ensembles 17A, 17B sensibles à la température.

Ainsi, pendant une opération liée à l'utilisation de l'objet, par exemple vers la fin de celle-ci, les deux composants capacitifs sont chargés, à une valeur de
20 tension prédéterminée, par la source d'énergie électrique extérieure, via le microprocesseur 14. Lorsque la carte à microcircuit est découplée du serveur ou lecteur de carte ou autre entité, les deux composants capacitifs restent chargés mais commencent à se décharger au travers de leurs propres espaces diélectriques respectifs et, au fur et à mesure que le temps s'écoule, sans que la
25 carte à microcircuit soit utilisée, la charge résiduelle de chacun des composants capacitifs décroît mais différemment dans l'un ou l'autre, en raison des fuites différentes déterminées par construction.

Lorsque la carte est à nouveau couplée à une source d'énergie électrique extérieure à l'occasion d'une nouvelle utilisation de l'objet, les charges
30 résiduelles des deux composants capacitifs sont représentatives du même intervalle de temps qu'on cherche à déterminer mais différent en raison des variations de température qui ont pu se produire pendant toute cette période de temps.

5 Au moment de la réutilisation de l'objet, les deux transistors à effet de champ de ces deux sous-ensembles sont alimentés et les valeurs des courants de drain sont lues et traitées par le microcircuit. Pour chaque couple de valeurs de courant de drain, le microcircuit va chercher en mémoire, dans le tableau T mentionné précédemment, la valeur de temps correspondante. Cette valeur de temps est alors comparée à la durée de vie V et l'utilisation de l'objet n'est autorisée que si le temps écoulé est inférieur à la durée de vie V.

10 En variante, cette valeur de temps peut être comparée avec une valeur disponible dans le serveur ou lecteur de carte ou autre entité, de préférence sécurisée. De plus, l'utilisation de l'objet peut n'être autorisée que si, non seulement le temps écoulé respecte la durée de vie de l'objet, mais si en outre, la valeur de temps obtenue dans la carte (par exemple la valeur de temps mémorisée dans le tableau T) est compatible avec la valeur disponible dans le serveur ou lecteur de carte ou autre entité, c'est-à-dire si en outre ces deux
15 valeurs coïncident ou sont relativement proches, selon une tolérance choisie au préalable.

Il n'est pas nécessaire de mémoriser le tableau T. Par exemple, le module de traitement, c'est-à-dire essentiellement le microprocesseur 14, peut comporter une partie de logiciel de calcul d'une fonction prédéterminée permettant de déterminer ladite information sensiblement indépendante des apports calorifiques en fonction des deux mesures.
20

Le troisième sous-ensemble 17C comporte, comme décrit plus haut, un espace diélectrique extrêmement mince le rendant insensible aux variations de température.

25 D'autres variantes sont possibles. En particulier, si on veut simplifier le sous-ensemble 17, on peut envisager de supprimer le composant capacitif 20 en tant que tel, car le transistor 30 à effet de champ peut lui-même être considéré comme un composant capacitif avec la grille 28b et le substrat 36 en tant qu'armatures, ces dernières étant séparées par l'espace diélectrique 34. Dans ce
30 cas, on peut considérer que le composant capacitif et l'unité de mesure sont confondus.

Il existe plusieurs possibilités pour conserver l'indication de temps entre les utilisations successives de l'objet.

Une première possibilité consiste à charger la cellule qui mesure le temps une fois, lors de la création de l'objet. Lorsqu'une opération liée à l'utilisation de l'objet (qui peut aussi être la création de l'objet) est effectuée, l'état de la charge de la cellule à un instant t_1 est mémorisé (par exemple inscrit dans un fichier
 5 d'une région sécurisée de la mémoire de l'entité électronique). Lors d'une nouvelle utilisation de l'objet, l'état de la charge de la cellule à l'instant t_2 est mémorisé (dans l'exemple, inscrit dans le fichier), et ainsi de suite, de façon que, lorsqu'une $N^{\text{ème}}$ utilisation a lieu, l'état de la charge de la cellule à l'instant t_N est mémorisé (dans l'exemple, t_{50} est inscrit dans le fichier).

10 Pour déterminer le temps écoulé entre la $1^{\text{ère}}$ et la $N^{\text{ème}}$ utilisations, il suffit de comparer l'état de la charge de la cellule à t_1 à l'état de la charge de la cellule à t_N . Par soustraction des valeurs des charges et par l'intermédiaire d'une table de correspondance entre charges et temps écoulé (pouvant être élaborée à partir d'un tableau analogue au tableau T décrit plus haut), on obtient le temps
 15 écoulé recherché.

En effet, par "charge" de la cellule, on entend ici la valeur physique liée à cette cellule, telle que la tension à ses bornes. Néanmoins, pour une utilisation plus simple de cette grandeur, on peut prévoir dans la carte un système (comme par exemple la table de correspondance mentionnée ci-dessus) permettant
 20 d'associer cette valeur physique à une grandeur logique plus directement représentative du temps.

D'autres possibilités consistent à recharger la cellule à intervalles de temps réguliers, ou encore à chaque mise sous tension de l'entité électronique sécurisée.

25 On utilise avantageusement un seul composant capacitif pour une pluralité d'utilisations d'un même objet. A chaque utilisation, le temps écoulé depuis la dernière recharge du composant capacitif est mesuré, puis le composant capacitif est rechargé. On accumule les temps ainsi mesurés dans un emplacement de la mémoire non volatile de l'entité électronique.

30 Cet emplacement mémoire mémorise ainsi le temps écoulé depuis la première charge du composant capacitif (la première charge ayant lieu, par exemple, lors de la création de l'objet) et permet de connaître le temps écoulé à tout moment.

Cette solution a pour avantage d'utiliser un seul composant capacitif ayant une épaisseur d'oxyde relativement faible, ce qui confère une plus grande précision dans la mesure du temps, par comparaison avec le cas d'un seul composant pour toute la durée de vie de l'entité électronique.

5 Le temps qui s'écoule entre l'instant de mesure de la charge du composant capacitif et le moment de sa recharge est parfois non négligeable. Pour prendre en compte cet intervalle de temps, on peut utiliser un second composant dont la fonction sera de prendre le relais du premier pendant cet intervalle de temps.

10 On peut également prévoir d'utiliser des composants capacitifs de précisions différentes afin d'améliorer la précision de la mesure : on choisira, parmi plusieurs mesures, celle obtenue à partir du composant le plus précis qui n'est pas déchargé.

15 Encore une autre possibilité consiste à recharger la cellule à chaque exécution, par l'objet considéré, d'une opération d'un type donné, après avoir mesuré le temps écoulé depuis la précédente opération du même type. Un avantage de cette possibilité est qu'on peut prévoir des composants adaptés à l'opération en question, pour améliorer la précision de la mesure du temps ; dans la cellule de mesure du temps, en particulier pour ce qui concerne l'épaisseur d'oxyde, on a vu par le tableau donné plus haut que le choix de l'épaisseur d'oxyde influe sur la précision de la mesure.

20 Cette possibilité de rechargement de la cellule à chaque exécution d'une opération d'un type donné est appropriée lorsqu'on prévoit une cellule de mesure du temps pour chaque application considérée dans l'entité électronique. En effet, sachant que la cellule est rechargée à chaque nouvelle utilisation de l'objet, chaque application ayant recours au système de gestion du temps conforme à la présente invention utilise la cellule de mesure du temps qui lui est associée.

25 Dans cette hypothèse, pour l'application considérée, la différence entre la charge maximale de la cellule et l'état de la charge à l'instant de la nouvelle utilisation est mémorisée (dans l'exemple, dans un fichier d'une région sécurisée de la mémoire de l'entité électronique). Cette différence représente le temps écoulé entre les deux utilisations.

30

Pour obtenir le temps écoulé entre la date de référence Dref et la N^{ème} utilisation de l'objet, il suffit alors d'additionner les (N-1) valeurs des différences précédemment mémorisées.

D'autres variantes, à la portée de l'homme du métier, sont possibles.

- 5 Ainsi, conformément à l'invention, l'utilisation du compteur de temps à l'intérieur de la carte permet d'améliorer la sécurité puisque le décompte du temps est difficile à falsifier.

REVENDICATIONS

5 1. Entité électronique sécurisée (11) comportant des moyens (23) adaptés à mémoriser au moins un objet, caractérisée en ce qu'elle contient un moyen (18) de mesure du temps qui s'écoule à partir d'une date de référence (Dref) associée audit objet et en ce qu'elle comporte :

10 - un moyen (19) de mémorisation d'une durée de vie (V) attribuée audit objet, le moyen (19) de mémorisation coopérant avec le moyen (18) de mesure du temps de façon à comparer, à chaque utilisation de l'objet, le temps écoulé et ladite durée de vie (V) et

- des moyens (21) de mise à jour et d'invalidation, pour mettre à jour ladite durée de vie ou rendre l'objet temporairement ou définitivement inutilisable s'il résulte de ladite comparaison que le temps écoulé atteint ou dépasse la durée de vie (V).

15 2. Entité électronique sécurisée (11) selon la revendication 1, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps qui s'écoule à partir de la date de référence (Dref) lorsque l'entité électronique (11) n'est pas alimentée par une source d'énergie extérieure.

20 3. Entité électronique sécurisée (11) selon la revendication 1, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps qui s'écoule à partir de la date de référence (Dref) lorsque l'entité électronique (11) n'est pas alimentée électriquement.

25 4. Entité électronique sécurisée (11) selon la revendication 1, 2 ou 3, caractérisée en ce que le moyen (18) de mesure du temps est adapté à fournir une mesure du temps qui s'écoule à partir de la date de référence (Dref) indépendamment de tout signal d'horloge extérieur.

5. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (18) de mesure du temps comporte un moyen de comparaison de deux dates.

30 6. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que le moyen (19) de mémorisation de la durée de vie (V) comporte une entité sécurisée et est situé dans ou hors de ladite entité électronique (11).

7. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que l'objet est un microcircuit, un code secret, un fichier ou un système de fichiers, une fonction cryptographique, une application ou des droits d'accès.

5 8. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce que la date de référence (Dref) est la date de création de l'objet.

9. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'elle comporte au moins un
10 sous-ensemble (17) comprenant :

un composant capacitif (20) présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et

15 un moyen (22) de mesure de la charge résiduelle du composant capacitif (20), ladite charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif (20) a été découplé de la source d'énergie électrique.

20 10. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce qu'elle comporte un moyen de commutation pour découpler ledit composant capacitif (20) de ladite source d'énergie électrique.

11. Entité électronique sécurisée (11) selon la revendication 9 ou 10, caractérisée en ce que ledit moyen (22) de mesure de la charge résiduelle est compris dans ledit moyen (18) de mesure du temps.

25 12. Entité électronique sécurisée (11) selon la revendication 9, 10 ou 11, caractérisée en ce que le composant capacitif (20) est une capacité réalisée suivant la technologie MOS et dont l'espace diélectrique est constitué par un oxyde de silicium.

30 13. Entité électronique sécurisée (11) selon l'une quelconque des revendications 9 à 12, caractérisée en ce que le moyen (22) de mesure de la charge résiduelle comprend un transistor (30) à effet de champ ayant une couche isolante (34), en ce que le composant capacitif (20) comporte une couche isolante (24) et en ce que l'épaisseur de la couche isolante (34) du

transistor (30) à effet de champ est notablement plus grande que l'épaisseur de la couche isolante (24) du composant capacitif (20).

5 14. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que l'épaisseur de la couche isolante (24) du composant capacitif (20) est comprise entre 4 et 10 nanomètres.

15 15. Entité électronique sécurisée (11) selon la revendication 12, 13 ou 14, caractérisée en ce qu'elle comporte :

au moins deux sous-ensembles (17A, 17B) comprenant chacun :

10 un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et

15 un moyen de mesure de la charge résiduelle du composant capacitif, ladite charge résiduelle étant au moins en partie représentative du temps qui s'est écoulé après que le composant capacitif a été découplé de la source d'énergie électrique,

lesdits sous-ensembles (17A, 17B) comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs,

20 et en ce que ladite entité électronique sécurisée (11) comporte en outre :

des moyens (14, 15, T) de traitement des mesures des charges résiduelles respectives desdits composants capacitifs, pour extraire desdites mesures une information sensiblement indépendante des apports calorifiques appliqués à ladite entité (11) pendant le temps écoulé à partir de la date de référence (Dref).

25 16. Entité électronique sécurisée (11) selon la revendication précédente, caractérisée en ce que lesdits moyens (14, 15, T) de traitement comportent un logiciel de calcul d'une fonction prédéterminée pour déterminer ladite information sensiblement indépendante des apports calorifiques en fonction desdites mesures.

30 17. Entité électronique sécurisée (11) selon l'une quelconque des revendications précédentes, caractérisée en ce qu'il s'agit d'une carte à microcircuit.

"Entité électronique sécurisée intégrant la gestion du temps de vie d'un objet"

ABREGE

Cette entité électronique sécurisée (11), adaptée à mémoriser au moins un objet, contient une unité (18) de mesure du temps qui s'écoule à partir d'une date de référence (Dref) associée à cet objet.

Elle comporte une unité (19) de mémorisation d'une durée de vie (V) attribuée à l'objet, coopérant avec l'unité (18) de mesure du temps de façon à comparer, à chaque utilisation de l'objet, le temps écoulé et la durée de vie (V).

Elle comporte aussi une unité (21) de mise à jour et d'invalidation, pour mettre à jour la durée de vie ou rendre l'objet temporairement ou définitivement inutilisable s'il résulte de la comparaison que le temps écoulé dépasse la durée de vie (V).

Applications notamment aux cartes à microcircuit du type cartes bancaires ou cartes SIM.

Figure 1.

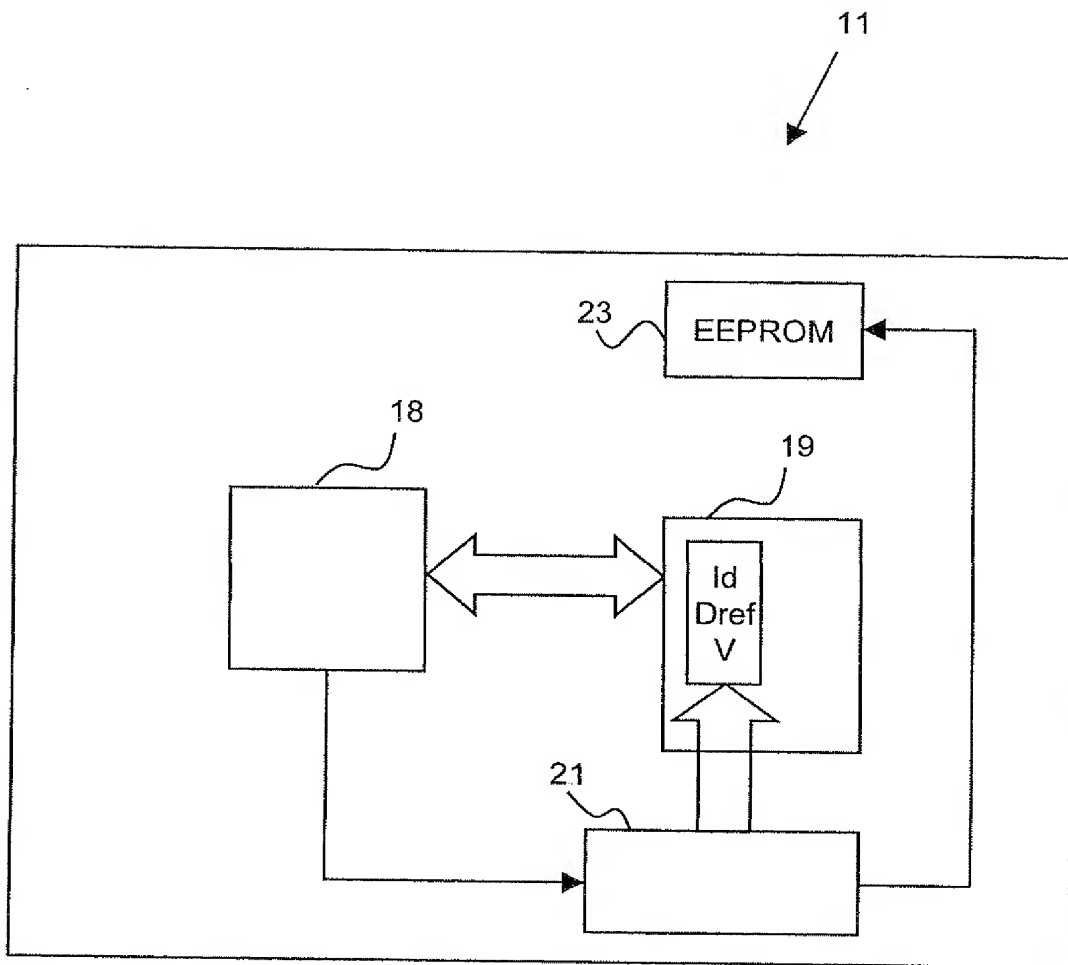


FIG. 1

FIG. 2

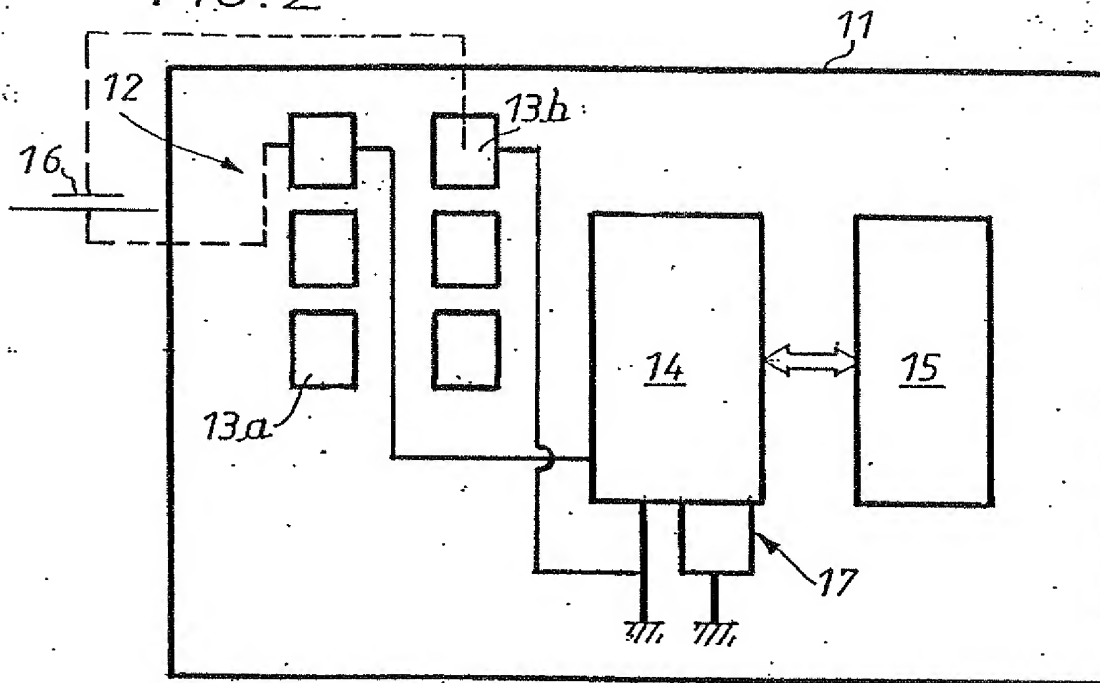


FIG. 3

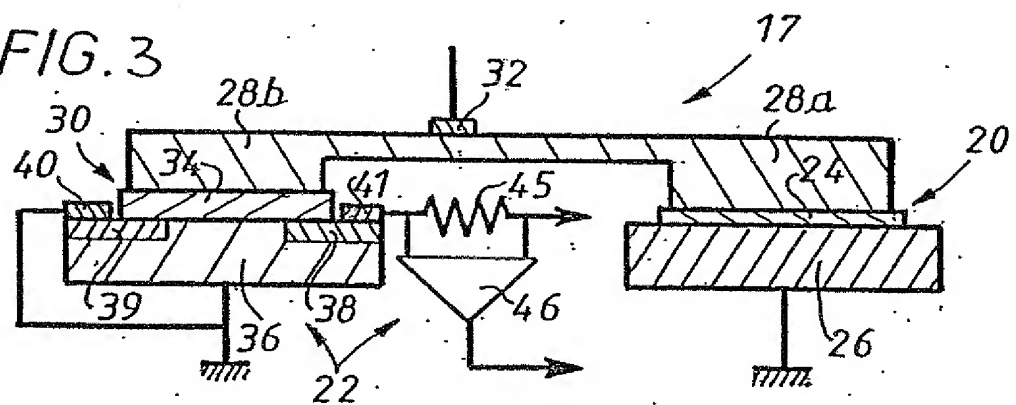
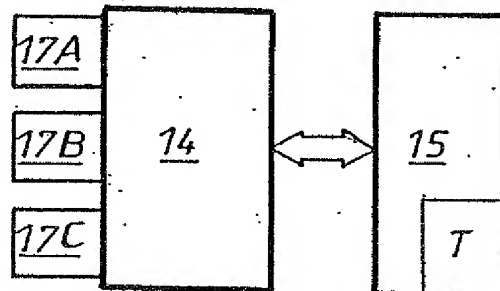


FIG. 4



Santarelli

Rémy, Santarelli & Cabinet Bonnet-Thirion

Conseils en Propriété Industrielle
European Patent, Trademark and Design Attorneys

Marc Santarelli ▲ ▲ ▲

Luc Santarelli ▲ ▲ ▲

Thierry Caen ▲ ▲ ▲

Laurence Julien-Raes ▲ ▲

François Lepelletier-Beaulord ▲ ▲ ▲

Herbert Lewitter ▲ ▲ ▲

Bruno Quantin ▲ ▲ ▲

Professeur Georges Bonet

Nathalie Bernat

Olivier Billot

Arnaud Bonmans ▲ ▲

Isabelle Clavier

Suzanne Luvost

Richard Compas ▲ ▲

Arnaud Delplanque

Marc Eluel

Sylvain Espinasse

Marta Fernandez Sanchez

Cédric Galup ▲ ▲

Michel George ▲ ▲

Guy Giraud

Julie Haller

Jean-Luc Hartmann ▲ ▲

Piotr Krolodziejczyk

Laurent Kunz ▲ ▲

Eric Le Bihan ▲ ▲

David Lefevre

Kerrie Milius ▲ ▲

Valérie Moncade ▲ ▲

Maurice Petit ▲ ▲

Pierre-Louis Renard

Léa Marie Rougemont

Muriel Rosenberg ▲ ▲

Helène Staroboff ▲ ▲

Carole Thirion ▲ ▲

Ghislain de Bernolles ▲

Catherine Ulinann ▲ ▲

▲ Conseil en Propriété Industrielle
Intellectual Property Attorneys

▲ Mandataire agréé auprès
de l'Office Européen des Brevets
European Patent Attorney

▲ Conseil Européen en Marque
European Trademark Attorney

Administration

Veronique Edmond

Isabelle Meyer

Monique Pourcin

Elisabeth Poulet

Secrétariat Général et finance

Dominique Lahauge

Siège social / Head office

14 avenue de la Grande Armée

Boîte Postale 227

75822 Paris Cedex 17

Tél +33 (0)1 40 55 43 43

Fax +33 (0)1 42 67 56 29

sio Conférence +33 (0)1 58 05 06 73

E-mail contact@santarelli.com

Bureau de Marseille

146 rue Paradis

13294 Marseille Cedex 6

Tél +33 (0)4 95 10 21 10

Fax +33 (0)4 95 10 21 10

E-mail marseille@santarelli.com

Bureau de Toulouse

Bureau Innocent A

Boîte Postale 388

31314 Labège Cedex

Tél +33 (0)5 61 00 75 30

Fax +33 (0)5 61 00 75 39

E-mail toulouse@santarelli.com

CERTIFIED TRANSLATION OF FRENCH DOCUMENTS

I, Jeremy WALKER, translator of Cabinet Santarelli, Conseils en Propriété Industrielle, 14, avenue de la Grande Armée 75017 Paris, France, hereby certify that I am fully conversant with the English and French languages and that I am a competent translator thereof, and I further certify that to the best of my knowledge and belief the following translations are true and accurate translations of the first draft document in the matter of French patent application number 02/14768, and of the cover letter forwarding that first draft document.


Signed on 23 July 2009



Jeremy WALKER

BY FAX
(28 pages)
01.41.38.17.02

Mr. Gérard GALAN
OBERTHUR CARD SYSTEMS SA
25 rue Auguste Blanche
B.P. 133
92800 PUTEAUX



Y/Ref. : GG/GG/02/278 CSP 0207
O/Ref. : BIF114644/FR – MR/alg

Re: CSP0207 - "Lifespan management of an object in the card"
Draft French national patent application
to be filed in the name of OBERTHUR CARD SYSTEMS SA

Inventors: Renan ABRALL, Bernard GEFROTIN

Dear Sir,

We have the pleasure in sending you herewith a copy of a first draft patent application (description, claims, abstract and informal drawings) intended to cover the above-identified invention.

We would invite you to study it attentively and to provide us with your comments at your earliest convenience.

In particular, we wish to know if the lifespan of the object must be understood as a total duration of actual use of the object, or rather as a period of time independent of the actual duration of use of the object (which could then "expire" without even having been used).

We look forward to receiving your observations, and trust you will receive this letter safely.

Yours faithfully,

CABINET BONNET-THIRION

Muriel ROSENBERG

Encl. draft patent application (description: pages 1 to 21; claims: pages 22 to 24;
abstract: 1 page; drawings: 2 pages of informal drawings)

SECURE ELECTRONIC ENTITY INTEGRATING OBJECT LIFESPAN MANAGEMENT

5 The invention relates to a secure electronic entity adapted to store one or more objects and in particular seeks to improve this kind of electronic entity so that it is able to manage a lifespan assigned to the object, running from a reference point in time associated with the object.

10 References hereinafter to managing time "in" the electronic entity mean management independent of any external time measuring system, for example a clock signal generator or any other means of measuring time external to the electronic entity.

 These specific features make the electronic entity of the present invention relatively inviolable.

15 The invention may be applied to any secure electronic entity, for example a secure microcircuit card including means enabling it to be coupled at least temporarily to an electrical power supply to carry out one or more operations. The invention can in particular be used to manage the lifespan of the card itself or of objects contained in the card in the absence of a continuous power supply.

20 The security of an object stored in an electronic entity (for example a microcircuit card such as a bank card, an access control card or other card) may be improved if it is possible to take account of the time that has elapsed since a reference point in time related to that object, whether the object is the microcircuit of the card itself or contained in the card, as is the case for a
25 secret code (PIN number), a data file, a cryptographical function (key, certificate), an application or access rights.

 A great variety of attacks are possible against microcircuit cards. The object of some of these attacks is to find the secrets stored in the memory of the microcircuit or to modify the normal behavior of the card in order to take
30 advantage thereof. For example, DPA (Differential Power Analysis), SPA (Simple Power Analysis), EMA (ElectroMagnetic Analysis), DEMA (Differential ElectroMagnetic Analysis), and DFA (Differential Fault Analysis) are well-known names for such attacks, referred to as non-intrusive, since they do not lead to the destruction of the card.

35 Nevertheless, as regards known microcircuit cards, the concept of

time is most often provided by the exterior (for example, conventionally, by an external clock signal), which makes the above-mentioned attacks easier to carry out.

5 An object of the present invention is to remedy these drawbacks by preventing an attacker fraudulently using a secure electronic entity or one or more objects stored therein. To this end, the present invention integrates into the electronic entity management of the assigned lifespan of the object or objects concerned or even of the electronic entity itself.

10 To this end, the invention provides a secure electronic entity including a unit adapted to store one or more objects, which entity is noteworthy in that it includes a unit for measuring the time that has elapsed since a reference point in time associated with that object and in that it contains:

15 - a unit for storing a lifespan assigned to the object, the storage unit co-operating with the time measuring unit to compare, at each use of the object, the elapsed time and the lifespan, and

- an updating and invalidation unit for updating the lifespan of the object or to render the object temporarily or permanently unusable if said comparison shows that the elapsed time has reached or passed the lifespan.

20 According to the invention, the means for determining the elapsed time from the reference point in time are situated in the electronic entity, which makes it more secure.

25 The time measuring unit is advantageously adapted to provide a measurement of the time that has elapsed since the reference point in time even when the electronic entity is not supplied with power by an external power supply.

The time measuring unit is advantageously adapted to supply a measurement of the time that has elapsed since the reference point in time even when the electronic entity is not supplied with electrical power.

30 The time measuring unit is advantageously adapted to supply a measurement of the time that has elapsed since the reference point in time independently of any external clock signal.

In this sense, the electronic entity is autonomous both from the time measurement point of view and from the electrical power supply point of view.

35 Alternatively, a battery and/or a clock can be provided in the electronic entity, of course.

The time measuring unit may include means for comparing two points in time, a point in time generally being an expression of the current time, and the two points in time being understood in the present context as being two moments in time defined relative to the same time reference, for example the
5 reference point in time associated with the object whose lifespan is monitored by the electronic entity. The comparison means may compare the current point in time directly to the reference point in time of the object, which means that the remaining lifespan of the object may be deduced directly, or at another time, such as the last time at which the object was used.

10 The unit for storing the lifespan advantageously includes a secure entity and may be situated inside or outside the electronic entity.

As mentioned in the introduction, by way of non-limiting example, the object may be a microcircuit, a secret code, a file or a file system, a cryptographic function such as a key or a certificate, an application or
15 access rights. The reference point in time associated with the object may be the point in time at which the object was created in the electronic entity.

In a preferred embodiment of the present invention, the secure electronic entity includes one or more subsystems comprising:

- a capacitive component subject to leakage across its dielectric space,
20 means being provided for coupling said capacitive component to an electrical power supply to be charged by the electrical power supply, and
- means for measuring the residual charge in the capacitive component, said residual charge being at least in part representative of the time that has elapsed since the capacitive component was decoupled from the electrical
25 power supply.

In this case, the capacitive component of the subsystem cited above can be charged only when the secure electronic entity is coupled to the electrical power supply, which may be external to the secure electronic entity, although that is not essential; the electronic entity may instead be supplied
30 with power by a battery in or on it.

The electronic entity may be provided with switching means for decoupling the capacitive component from the electrical power supply, this event initializing the time measurement.

More generally, measurement of time, i.e. variation of the charge in
35 the capacitive component, begins, after it has been charged, as soon as the

component is electrically insulated from any other circuit and can be discharged only across its own dielectric space.

5 However, even if the residual charge measured is physically linked to the time that has elapsed between isolating the capacitive component and a given measurement of its residual charge, a measured time interval may be determined between two measurements, the first measurement determining a reference residual charge, as it were. The means for measuring the residual charge in the capacitive component are used to determine an elapsed time.

10 The capacitive component is charged during use of the object whose lifespan is monitored by the electronic entity, the term "use" being understood in the widest sense and including, for example, the creation of the object. During such use the means for measuring the residual charge are implemented to provide information that is at least partially representative of the elapsed time since the last use..

15 Moreover, the invention further enables the secure electronic entity to continue to measure the elapsed time even after it has been temporarily supplied with power and has then been deprived of any further electrical power supply. Thus the invention does not necessitate the use of a continuous electrical power supply.

20 The means for measuring the residual charge may be included in the time measuring unit referred to above.

In a preferred embodiment, the means for measuring the residual charge comprise a field-effect transistor whose gate is connected to a terminal of the capacitive component, i.e. to a "plate" of a capacitor.

25 A capacitor of the above kind may be implemented in the MOS technology and its dielectric space may then consist of a silicon oxide. In this case, it is advantageous for the field-effect transistor also to be implemented in the MOS technology. The gate of the field-effect transistor and the "plate" of the MOS capacitive component are connected together and constitute a kind of a floating gate that may be connected to a component for injecting charge carriers.

30 There may also be no electrical connection as such with the external environment. The connection of the floating gate may be replaced by an (electrically insulative) control gate that charges the floating gate, for example by means of a tunneling effect or "hot carriers". The gate causes charge

35

carriers to migrate toward the floating gate common to the field-effect transistor and the capacitive component. This technique is well known to EPROM and EEPROM manufacturers.

5 The field-effect transistor and the capacitive component may constitute a unit integrated into a microcircuit contained in the secure electronic entity or forming part of another microcircuit housed in the same secure electronic entity.

10 During certain operations linked to a use of the object whose lifespan is monitored by the secure electronic entity, when the secure electronic entity is coupled to an external electrical power supply, the capacitive component is charged to a predetermined value, which is either known or measured and stored, and the means for measuring the residual charge are connected to a terminal of the capacitive component.

15 At the end of a series of operations corresponding to a period of use of the object, the means for measuring the residual charge, and in particular the field-effect transistor, are no longer supplied with power, but its gate connected to the terminal of the capacitive component is brought to a voltage corresponding to the charge therein.

20 During the whole of the period between the reference point in time associated with the object and the point in time of its current use, the capacitive component is slowly discharged across its own dielectric space with the result that the voltage applied to the gate of the field-effect transistor is progressively reduced.

25 When the electronic entity is again connected to an electrical power supply to carry out a new operation linked to a new period of use of the object, an electrical voltage is applied between the drain and the source of the field-effect transistor. This generates an electric current from the drain to the source (or in the opposite direction, as appropriate), which current may be collected and analyzed.

30 The value of the measured electrical current depends on the technological parameters of the field-effect transistor, on the potential difference between the drain and the source, and the voltage between the gate and the substrate. The current therefore depends on the charge carriers accumulated in the floating gate common to the field-effect transistor and to
35 the capacitive component. Consequently, that drain current is also

representative of the elapsed time, on use of the object, between the reference point in time and the current point in time.

5 The leakage current of the above kind of capacitor depends of course on the thickness of its dielectric space and on other technological parameters such as the contact lengths and areas of the elements of the capacitive component. It is also necessary to take into account the three-dimensional architecture of the contacts between these parts, which may induce phenomena modifying the parameters of the leakage current (for example, modification of the tunnel capacitance). The type and quantity of dopants and defects may be modulated to modify the characteristics of the leakage current.

10 Temperature variations, to be more precise the average of the calorific energy input to the secure electronic entity during the time of use of the object, also have an influence. In fact, any parameter intrinsic to the MOS technology may be a source of modulation of the time measurement process.

15 The thickness of the insulative layer of the field-effect transistor is advantageously significantly greater (for example approximately three times) than the thickness of the insulative layer of the capacitive component.

20 The thickness of the insulative layer of the capacitive component is advantageously from 4 nanometers to 10 nanometers.

To obtain information that is representative substantially of only time, in another embodiment, at least two subsystems as defined herein above may be operated "in parallel". The two temperature-sensitive capacitive components are designed with different leaks, all other things being equal, i.e. their dielectric spaces (the thickness of the silicon oxide layer) have different thicknesses.

To this end, in one advantageous embodiment of the invention, the electronic entity defined hereinabove is noteworthy in that it includes:

30 at least two of the previously mentioned subsystems each comprising:
a capacitive component subject to leakage across its dielectric space, means enabling said capacitive component to be coupled to an electrical power supply in order to be charged by said electrical power supply, and

35 means for measuring the residual charge in the capacitive component said residual charge being at least in part representative

of the time which has elapsed after the capacitive component was decoupled from the electrical power supply, said subsystems comprising capacitive components having different leaks across their respective dielectric spaces,

5 and in that said secure electronic entity further includes:

means for processing the measurements of the respective residual charges in said capacitive components to extract from said measurements information substantially independent of heat input to said secure electronic entity during the time that has elapsed since the reference point in time.

10 For example, the processing means may include a table of stored time values addressed by the respective measurements. In other words, each pair of measurements designates a stored time value independent of temperature and temperature variations during the measured period. The electronic entity advantageously includes a memory associated with a
15 microprocessor and a portion of that memory may be used to store the table of values.

Alternatively, the processing means may include calculation software programmed to execute a predetermined function for calculating time information, substantially independent of calorific input, as a function of the
20 two measurements cited above.

The invention is particularly suitable for application to microcircuit cards. The secure electronic entity may be a microcircuit card, or include one, or may be of another type, for example a PCMCIA (Personal Computer Memory Card International Architecture) card.

25 The invention is also noteworthy by virtue of its level of integration.

Further aspects and advantages of the invention will become apparent on reading the following detailed description of particular embodiments of the invention, provided by way of non-limiting example. The description refers to the accompanying drawings, in which:

- 30 - Figure 1 is a block diagram of one particular embodiment of a secure electronic entity conforming to the present invention;
- Figure 2 is a block diagram of a microcircuit card to which one particular embodiment of the invention may be applied;
- Figure 3 is a theoretical diagram of a subsystem that one particular
35 embodiment of the secure electronic entity may include; and

- Figure 4 is a block diagram of a variant of the embodiment shown in Figures 1 and 2.

As shown in **Figure 1**, in one particular embodiment, a secure electronic entity 11 conforming to the present invention includes a non-volatile memory 23, for example of the EEPROM type, storing data relating to one or more objects, such as a microcircuit, a secret code (PIN or other), a file or a system of files, an encryption key or a certificate, an application or access rights.

The electronic entity 11 contains a unit 18 for measuring the time that elapses from a reference point in time Dref associated with the object stored in the EEPROM 23. The reference point in time may be the point in time the object was created in the card, for example.

The time measuring unit 18 is independent of any external time measuring system, for example a clock signal generator or other means of measuring time external to the card.

The secure electronic entity 11 also includes a unit 19 for storing a plurality of parameters defining the object whose lifespan is to be managed in the secure electronic entity:

- an identifier Id of the object,
- the above reference point in time Dref, and
- a predetermined lifespan V assigned to the object.

The operations that create an object naturally use secure mechanisms to protect the "lifespan" data item V.

The storage unit 19 with the EEPROM 23 may constitute a single memory and is advantageously a secure memory of the electronic entity 11 that in particular is not accessible from the outside. Alternatively, the storage unit 19 may be outside the secure electronic entity 11, in a secure external entity. In this case, the value of the lifespan V is received from the outside, from a "trusted" third party (approved authority) by the secure electronic entity 11, by means of a secure protocol (i.e. a protocol employing cryptography) and is stored at least temporarily in a secure area of the electronic entity 11.

The secure electronic entity 11 further includes an updating and invalidation unit 21 controlled by the time measuring unit 18.

In accordance with the present invention, the storage unit 19 cooperates with the time measuring unit 18 to compare, on each use of the

object, the elapsed time and the lifespan V.

If, after comparing the elapsed time and the lifespan V, it is apparent that the lifespan has been reached or passed, the updating and invalidation unit 21 acts on the object, either to update its lifespan V in the storage unit 19, in order to extend the lifespan of the object, subject to the use of security mechanisms, or to inhibit the functioning of the object temporarily, for a predetermined time period, or even to render the object permanently unusable.

A region (for example a file) containing the point in time, for example in seconds, since the reference point in time Dref may be provided in the memory of the secure electronic entity 11.

Thereafter, before authorizing new use of the object, the point in time of the current use is compared with the reference point in time Dref. If the difference between the two points in time is equal to or greater than the lifespan V, the updating and invalidation unit 21 comes into action.

The invention has many possible applications, including:

- limiting the lifespan of a microcircuit card as a function of the term of the agreement entered into by its user, to guarantee no hijacking and fraudulent use of the card beyond the intended time of use;
- limiting the lifespan of a file system, in a similar manner;
- commanding a periodic change by the user of the confidential code associated with use of the secure electronic entity;
- defining when the validity of data contained in a file expires, after which reading of the data is rendered impossible or is at least accompanied by a warning to the user;
- defining when the validity of an application expires, for example in the case of an application linked to a sporting, cultural or artistic event that is time-limited, after which the application is automatically eliminated;
- defining when a free trial period of an on-line evaluation version of software ends, after which the rights to use the software may be extended (subject to the use of a security mechanism) after payment by the user;
- managing electronic access rights to a piece of music, a film or the like via the Internet, in the form of a fixed-charge subscription of predetermined duration (for example one month) or as a function of the real time of use of the access rights (for example ten hours of listening);

- and so on.

In the final application example referred to above, a user wishes to access the content of the Internet site of a musical content publisher for a defined time period, for example. To this end he purchases access rights to the musical content for a particular period, for example four hours. After
5 verification, the publisher sends the secure electronic entity of the user a secure message granting listening rights for the intended time period. On receiving this message, the secure electronic entity creates in its memory a "listening right" object and initializes the lifespan V with the chosen value,
10 here four hours.

On the first use of the object, i.e. on the first access to the musical content, the secure electronic entity verifies the presence of the "listening right" object and stores the point in time at which listening begins. The user then accesses the musical content. On each request for secret decryption
15 data, the secure electronic entity verifies the presence of the "listening right" object and its validity as a function of the updated time. If the difference between the current point in time and the reference point in time (which in this example is the point in time at which listening begins) is greater than four hours, the right is still valid and the secure electronic entity supplies the secret
20 data, which is used to decrypt the musical content. On the other hand, if that difference is equal to or greater than four hours, the right is no longer valid and the secret decoding data is not supplied. The electronic entity can also invalidate the "listening right" object temporarily, or even destroy it.

If the user stops using the "listening right" object before the right
25 expires, the lifespan of the object is updated as a function of the remaining time: the new value of the lifespan is equal to the previous lifespan less the current point in time and the point in time at which listening began.

In another example of an application of the invention, in the field of mobile telecommunications, the secure electronic entity may be a smart card
30 of the SIM card type and the object may be an SAT (SIM application toolkit) application as defined in particular by the GSM 03.48 standard. The applications may be loaded at the time of customizing the SIM card or downloaded, either using the SMS (Short Message Service) technology, also defined by the GSM standard cited above, or via a reader connected to a
35 computer in turn connected to a card management center.

The electronic entity manages a table of SAT applications containing, for each application, an identifier AID of the application, a reference point in time (for example the point in time the application was created), and the lifespan of the application.

5 Each time the application is started, the SIM card uses the time counter to determine if the application is still valid. If not, i.e. if the difference between the current point in time and the point in time the application was created is equal to or greater than the lifespan of the application, the card sends a Delete_application (AID) type administrative command and updates
10 the table of SAT applications.

Figure 2 shows one particular embodiment of a secure electronic entity 11 conforming to the present invention taking the form of a microcircuit card. The secure electronic entity 11 includes a unit 12 for coupling it to an external electrical power supply 16.

15 In the particular embodiment shown, the secure electronic entity 11 includes metal connection areas adapted to be connected to a unit forming a card reader. Two of these connection areas 13a, 13b are reserved for supplying electrical power to the microcircuit, the electrical power supply being in a server or other device to which the secure electronic entity is
20 momentarily connected. These connection areas may be replaced by an antenna housed in the thickness of the card and adapted to supply the microcircuit with the electrical energy it needs as well as providing bidirectional transmission of radio-frequency signals for exchanging information. This is known as contactless technology.

25 The microcircuit comprises a microprocessor 14 conventionally associated with a memory 15.

One particular embodiment of the secure electronic entity 11 includes at least one time measuring subsystem 17 (or is associated with at such a subsystem) given the task of measuring time.

30 The subsystem 17, which is shown in more detail in Figure 3, is therefore accommodated in the secure electronic unit 11. It may form part of the microcircuit and may be implemented in the same integration technology as the microcircuit.

35 In the example, this subsystem 17 is connected to no internal electrical power supply. It can therefore only be powered when the secure

electronic entity 11 is actually coupled to a server or to a card reader, comprising such an of electrical power supply. However, if the secure electronic entity 11 is to be continuously powered, the subsystem 17 which has the task of measuring time may or may not be powered via a switching unit enabling the secure electronic entity 11 to be coupled to the electrical power source or to isolate it therefrom. Such a switching unit is for example an integral part of the microprocessor 14, or is constituted by switching elements managed by the microprocessor 14.

The subsystem 17 comprises a capacitive component 20 subject to leakage across its dielectric space 24 and a unit 22 for measuring the residual charge in the component 20.

The residual charge is at least in part representative of the time elapsed since the capacitive component 20 was decoupled from the electrical power supply, that is to say, in the present example, from the reference point in-time Dref associated with the object whose lifespan is to be monitored.

The capacitive component 20 is charged by the external electrical power supply during an operation linked to the use of the object, either via a direct connection, as in the present example, or by any other means for charging the gate. The tunnel effect is one method of charging the gate with no direct connection. In the present example, the microprocessor 14 controls the charging of the capacitive component 20.

In the present example, the capacitive component 20 is an MOS technology capacitor. The dielectric space 24 of the capacitor consists of a layer of silicon oxide deposited on the surface of a substrate 26 constituting one plate of the capacitor. Here the substrate 26 is grounded, i.e. connected to one of the power supply terminals of the external electrical power supply when the latter is connected to the card. The other plate of the capacitor is a conductive deposit 28a applied to the other face of the layer of silicon oxide.

The measuring unit 22 mentioned above essentially comprises a field-effect transistor 30, here implemented in the MOS technology, like the capacitor. The gate of the transistor 30 is connected to a terminal of the capacitive component 20. In the example, the gate is a conductive deposit 28b of the same kind as the conductive deposit 28a which constitutes one of the plates of the capacitive component 20.

The two conductive deposits 28a and 28b are connected together or

constitute a single conductive deposit. A connection 32 connected to the microprocessor 14 is used to apply a voltage to the two deposits 28a and 28b for a short time interval to charge the capacitive component 20. The microprocessor 14 controls the application of this voltage.

5 More generally, the connection 32 is used to charge the capacitive component 20 at a given time under the control of the microprocessor 14, and the discharging of the capacitive component 20 across its dielectric space 24 begins when this charging connection is broken by the microprocessor 14 (or
10 when the secure electronic entity 11 as a whole is decoupled from any electrical power supply), this loss of electric charge being representative of the elapsed time. Measuring the time involves turning the transistor 30 on momentarily, which presupposes the presence of an electrical power supply between its drain and source.

15 The MOS technology field-effect transistor 30 includes, in addition to the gate, a gate dielectric space 34 separating the gate from a substrate 36, in which a drain region 38 and a source region 39 are defined. The gate dielectric space 34 consists of an insulative layer of silicon oxide. The source connection 40 applied to the source region 39 is grounded and connected to the substrate 36. The drain connection 41 is connected to a drain current
20 measuring circuit that includes a resistor 45 to opposite ends of which two inputs of a differential amplifier 46 are connected. The voltage delivered at the output of this amplifier is therefore proportional to the drain current.

25 The gate 28b is set to floating position during the time that elapses between two couplings or connections to an external electrical power source, i.e. when two successive uses of the object are made. In other words, no voltage is applied to the gate during this interval of time. On the other hand, because the gate is connected to one plate of the capacitive component 20, the gate voltage during this interval of time is equal to a voltage that develops
30 between the terminals of the capacitive component 20 and which is the result of an initial charging therein carried out under the control of the microprocessor 14 during the last use of the object.

35 The insulative layer of the transistor 30 is significantly thicker than that of the capacitive component 20. By way of non-limiting example, the thickness of the insulative layer of the transistor 30 may be about three times the thickness of the insulative layer of the capacitive component 20.

Depending on the application envisaged, the thickness of the insulative layer of the capacitive component 20 is from about 4 nanometers to about 10 nanometers.

When the capacitive component 20 is charged by the external electrical power supply, and after the charging connection has been broken at the command of the microprocessor 14, the voltage across the capacitive component 20 decreases slowly as the latter is progressively discharged across its own dielectric space 24. Given its thickness, the discharge across the dielectric space 34 of the field-effect transistor 30 is negligible.

By way of non-limiting example, for a given dielectric space thickness, if the gate and the plate of the capacitive component 20 are charged to 6 volts at a time $t = 0$, the time associated with a loss of charge of 1 volt, i.e. to a reduction of the voltage to 5 volts, is of the order of 24 seconds for a thickness of 8 nanometers.

The times for other thicknesses are set out in the following table:

Time	1 hour	1 day	1 week	1 month
Oxide thickness	8.17 nm	8.79 nm	9.17 nm	9.43 nm
Time accuracy	1.85%	2.09%	2.24%	3.10%

The accuracy depends on the error in reading the drain current (approximately 0.1%). Accordingly, to be able to measure times of the order of one week, a dielectric space layer thickness of the order of 9 nanometers may be required.

Figure 3 shows one particular architecture that uses a direct connection to the floating gate (28a, 28b) to apply an electric potential thereto and therefore to cause charges to transit. Another option is indirect charging, as mentioned above, by means of a control gate replacing the direct connection, using the technology employed to fabricate EPROM or EEPROM cells.

The Figure 4 variant provides three subsystems 17A, 17B, 17C each associated with the microprocessor 14. The subsystems 17A and 17B comprise capacitive components with relatively slow leakage to enable measurement of relatively long times.

However, these capacitive components are generally sensitive to

temperature variations. The third subsystem 17C includes a capacitive component having a very thin dielectric space (less than 5 nanometers thick). It is therefore insensitive to temperature variations. The two capacitive components of the subsystems 17A, 17B have different leakages across their
5 respective dielectric spaces.

Moreover, the secure electronic entity includes a module for processing respective residual charge measurements present in the capacitive components of the first two subsystems 17A, 17B. This processing module is adapted to extract from these measurements information that is
10 representative of time and substantially independent of heat input to the secure electronic entity during the time elapsed since the reference point in time.

In the present example, this processing module is lumped together with the microprocessor 14 and the memory 15. In particular, space is
15 reserved in the memory 15 for storing a double-entry table T of time values that is addressed by means of the respective measurements from the subsystems 17A and 17B. In other words, a portion of the memory includes a set of time values and each value corresponds to a pair of measurements resulting from reading the drain current of each of the two transistors of the
20 temperature-sensitive subsystems 17A, 17B.

Accordingly, during an operation linked to the use of the object, for example towards the end thereof, the two capacitive components are charged to a predetermined voltage by the external electrical power supply via the microprocessor 14. When the microcircuit card is decoupled from the server,
25 card reader or other entity, the two capacitive components remain charged but begin to discharge across their respective dielectric spaces and, as time passes without the microcircuit card being used, the residual charge in each of the capacitive components decreases, but differently in the two components, because of the different leakage rates resulting from their
30 respective designs.

When the card is again coupled to an external electrical power supply, for example on the occasion of a new use of the object, the residual charges in the two capacitive components are representative of the same
35 time interval to be determined, but different because of any temperature variations that may have occurred during this time period.

When the object is used again, the two field-effect transistors of the two subsystems are supplied with energy and the drain current values are read and processed by the microcircuit. For each pair of values of the drain current, the microcircuit looks for the corresponding time value in memory, in the table T mentioned above. That time value is then compared to the lifespan V and use of the object is authorized only if the elapsed time is less than the lifespan V.

Alternatively, this time value may be compared to a value available in the server, card reader or some other (and preferably secure) entity. Moreover, use of the object may be authorized only if the elapsed time respects the lifespan of the object and the time value obtained in the card (for example the time value stored in the table T) is compatible with the value available in the server or card reader or other entity, i.e. if the two values also coincide or are relatively close together, within a preselected tolerance.

It is not necessary to store the table T. For example, the processing module, i.e. essentially the microprocessor 14, may include software for calculating a predetermined function for determining said information as a function of the two measurements and substantially independently of the heat input.

As described above, the third subsystem 17C includes an extremely thin dielectric space making it insensitive to temperature variations.

Other variants are feasible. In particular, to simplify the subsystem 17, the capacitive component 20 as such may be eliminated, because the field-effect transistor 30 may be considered as a capacitive component with the gate 28b and the substrate 36 as its plates, separated by the dielectric space 34. In this case, the capacitive component and the measuring unit may be regarded as lumped together.

There are a number of options for preserving the time indication between successive uses of the object.

A first possibility is to charge the cell that measures time once, when the object is created. When an operation linked to the use the object (which may also be the creation of the object) is performed, the state of charge in the cell at a time t_1 is stored (for example written in a file in a secure area of the memory of the electronic entity). When a new use is made of the object, the state of charge of the cell at the time t_2 is stored (in the example, written in

the file), and so forth, such that, when an N^{th} use takes place, the state of charge of the cell at the time t_N is stored (in the example, t_{50} is written in the file).

5 To determine the time lapsed between the 1^{st} and N^{th} uses, it suffices to compare the state of charge of the cell at t_1 with the state of charge of the cell at t_N . By subtracting the values of the charges and using a look-up table relating charges to lapsed time (which may be produced on the basis of a table similar to table T described above), the sought lapsed time is obtained.

10 To be precise, "charge" of the cell is used here to mean the physical value linked to that cell, such as the voltage at its terminals. Nevertheless, for a simpler use of that quantity, provision may be made for a system in the card (such as the look-up table mentioned above) enabling that physical value to be associated with a logic quantity more directly representative of time.

15 Other possibilities consist of recharging the cell at regular intervals, or each time power is supplied to the secure electronic entity.

20 It is advantageous to use a single capacitive component for a plurality of uses of the same object. At each use, the time lapsed since the last recharge of the capacitive component is measured, then the capacitive component is recharged. The times so measured are accumulated in a non-volatile memory location of the electronic entity.

This memory location thus stores the time lapsed since the first charge of the capacitive component (the first charge taking place, for example, on creation of the object) and makes it possible to know the time lapsed at any moment.

25 This has the advantage of using a single capacitive component having a relatively thin oxide layer, which makes time measurement more accurate compared to using a single component for the whole of the lifespan of the electronic entity.

30 The time that elapses between the time of measuring the charge on the capacitive component and the time that it is recharged is sometimes non-negligible. To take account of this interval of time, a second component may be used whose function is to take over from the first during this time interval.

35 Capacitive components of different accuracy may also be used to improve the accuracy of the measurement; from a plurality of measurements, the measurement obtained from the most accurate component that has not

been discharged is chosen.

Still another possibility consists of recharging the cell each time an operation of given type is executed by the object considered, after having measured the time lapsed since the preceding operation of the same type. An advantage of this possibility is that components may be provided that are adapted to the operation in question, to improve the accuracy of the time measurement; in the time measurement cell, in particular as regards the thickness of the oxide, it was seen from the table given above that the choice of the thickness of the oxide affects the accuracy of the measurement.

This possibility of recharging the cell on each execution of an operation of a given type is appropriate when a time measuring cell is provided for each application considered in the electronic entity. Indeed, knowing that the cell is recharged on each new use of the object, each application using the time management system in accordance with the present invention uses the time measuring cell associated with it.

In such a case, for the application considered, the difference between the maximum charge of the cell and the state of charge at the time of the new use is stored (in the example, in a file of a secure area of the memory of the electronic entity). This difference represents the time lapsed between the two uses.

To obtain the time lapsed between the reference time D_{ref} and the N^{th} use of the object, it then suffices to add the $(N-1)$ values of the differences stored previously.

Other variants are possible that are within the capability of the person skilled in the art.

Thus, according to the invention, the use of the time counter within the card improves security since downcounting time is difficult to falsify.

CLAIMS

1. Secure electronic entity (11) including means (23) adapted to store one or more objects, which entity is characterized in that it includes a measuring means (18) for measuring the time that has elapsed from a reference point in time (Dref) associated with said object and in that it comprises:

- storage means (19) for storing a lifespan (V) assigned to said object, the storage means (19) co-operating with the time measuring means (18) to compare, at each use of the object, the elapsed time and said lifespan (V), and
- updating and invalidation means (21) for updating said lifespan of the object or to render the object temporarily or permanently unusable if said comparison shows that the elapsed time has reached or passed the lifespan (V).

2. Secure electronic entity (11) according to Claim 1, characterized in that the time measuring means (18) are adapted to provide a measurement of the time that has elapsed since the reference point in time (Dref) when the electronic entity (11) is not supplied with power by an external power supply.

3. Secure electronic entity (11) according to Claim 1, characterized in that the time measuring means (18) are adapted to supply a measurement of the time that has elapsed since the reference point in time (Dref) when the electronic entity (11) is not supplied with electrical power.

4. Secure electronic entity (11) according to Claim 1, 2 or 3, characterized in that the time measuring means (18) are adapted to supply a measurement of the time that has elapsed since the reference point in time (Dref) independently of any external clock signal.

5. Secure electronic entity (11) according to any one of the preceding claims, characterized in that the time measuring means (18) include means for comparing two points in time.

6. Secure electronic entity (11) according to any one of the preceding claims, characterized in that the means (19) for storing the lifespan (V) include a secure entity and are situated inside or outside said electronic entity (11).

7. Secure electronic entity (11) according to any one of the preceding claims, characterized in that the object is a microcircuit, a secret code, a file, a

file system, a cryptographical function, an application or access rights.

8. Secure electronic entity (11) according to any one of the preceding claims, characterized in that the reference point in time (Dref) is the point in time of creation of the object.

5 9. Secure electronic entity (11) according to any one of the preceding claims, characterized in that it includes one or more subsystems (17) comprising:

a capacitive component (20) subject to leakage across its dielectric space, means for coupling said capacitive component to an electrical power supply to be charged by said electrical power supply, and

10 means (22) for measuring the residual charge in the capacitive component (20), said residual charge being at least in part representative of the time that has elapsed since the capacitive component (20) was decoupled from the electrical power supply.

15 10. Secure electronic entity (11) according to the preceding claim, characterized in that it comprises a switching means to decouple said capacitive component (20) from said electrical power supply.

11. Secure electronic entity (11) according to the claim 9 or 10, characterized in that said means (22) for measuring the residual charge are included in said time measuring means (18).

20 12. Secure electronic entity (11) according to Claim 9, 10 or 11, characterized in that the capacitive component (20) is an MOS capacitor whose dielectric space consists of a silicon oxide.

13. Secure electronic entity (11) according to any one of Claims 9 to 25 12, characterized in that the means (22) for measuring the residual charge comprise a field-effect transistor (30) having an insulative layer (34), in that the capacitive component (20) includes an insulative layer (24), and in that the thickness of the insulative layer (34) of the field-effect transistor (30) is significantly greater than the thickness of the insulative layer (24) of the 30 capacitive component (20).

14. Secure electronic entity (11) according to the preceding claim, characterized in that the thickness of the insulative layer (24) of the capacitive component (20) is from 4 to 10 nanometers.

15. Secure electronic entity (11) according to Claim 12, 13 or 14, 35 characterized in that it includes:

at least two subsystems (17A, 17B) each comprising:

a capacitive component subject to leakage across its dielectric space,
means enabling said capacitive component to be coupled to an electrical
power supply in order to be charged by said electrical power supply, and

5 means for measuring the residual charge in the capacitive component,
said residual charge being at least in part representative of the time which has
elapsed after the capacitive component was decoupled from the electrical
power supply, said subsystems (17A, 17B) comprising capacitive components
having different leaks across their respective dielectric spaces,
10 and in that said secure electronic entity (11) further includes:

means (14, 15, T) for processing respective measurements of residual
charges in said capacitive components to extract from said measurements
information substantially independent of heat input to said entity (11) during
the time that has elapsed since the reference point in time (Dref).

15 16. Secure electronic entity (11) according to the preceding claim,
characterized in that said processing means (14, 15, T) include software for
calculating a predetermined function for determining said information as a
function of said measurements and substantially independently of heat input.

20 17. Secure electronic entity (11) according to any one of the
preceding claims, characterized in that it is a microcircuit card.

"Secure electronic entity integrating object lifespan management"

ABSTRACT

5

This secure electronic entity (11), adapted to store at least one object, contains a unit (18) for measurement of the time that elapses from a reference point in time (Dref) associated with that object.

10 It comprises a unit (19) for storing a lifespan (V) attributed to the object, cooperating with the time measuring unit (18) so as to compare, at each use of the object, the time lapsed and the lifespan (V).

It also comprises a unit (21) for updating and invalidating, to update the lifespan or make the object temporarily or permanently unusable if the comparison shows that the lapsed time exceeds the lifespan (V).

15 Applications in particular for microcircuit cards of the bank card or SIM card type .

Figure 1.

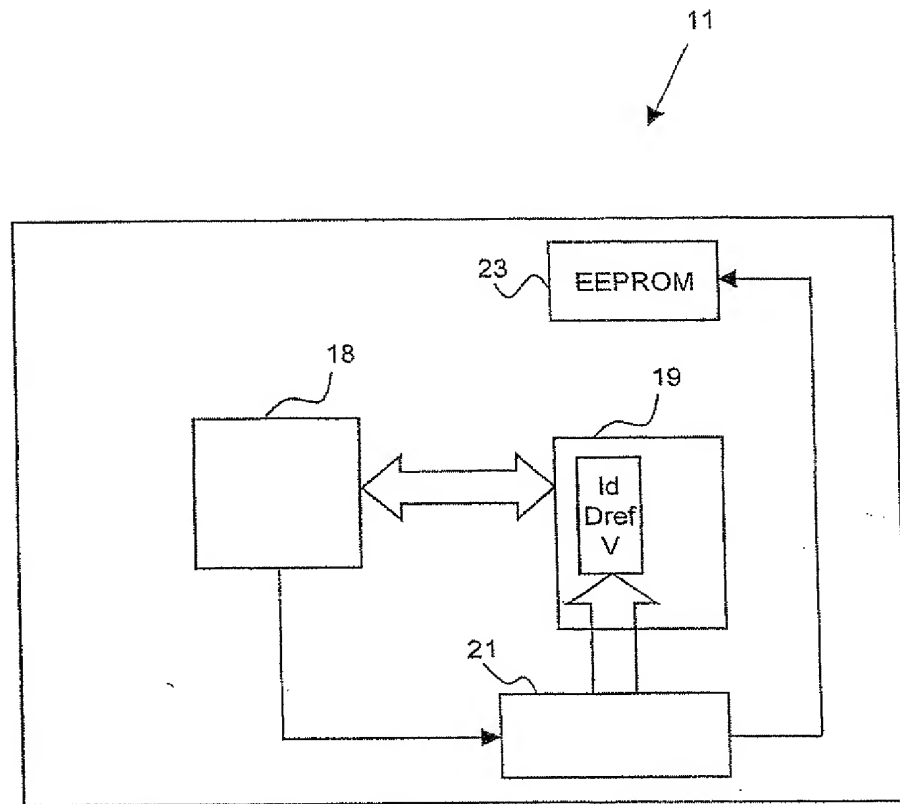


FIG. 1

Fig.2

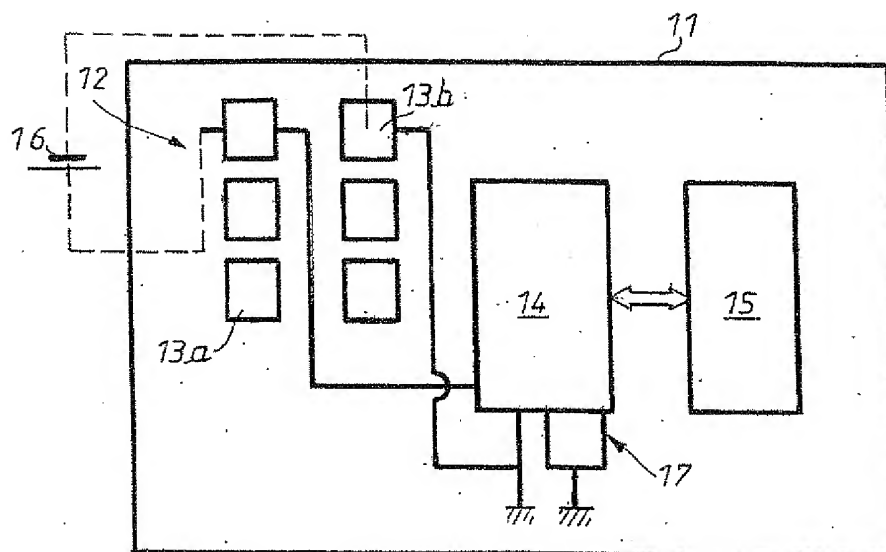


Fig.3

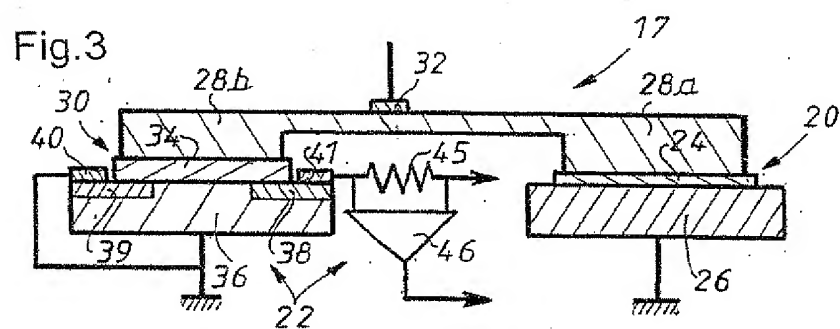


Fig.4

